FortiClient EMS - Administration Guide

VERSION 1.2.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 25, 2017

FortiClient EMS 1.2.0 Administration Guide

04-120-408881-20170725

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-06-15	Initial release
2017-06-22	New topic added for upgrading from earlier version of FortiClient EMS.
2017-07-10	Creating profiles to automatically upgrade FortiClient on page 56 added.
2017-07-25	Clarified when FortiClient EMS can be deployed with Windows workgroups.

Introduction

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoint devices (computers). FortiClient EMS provides an efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS is designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints. Some benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows PCs
- Updating profiles for endpoint users regardless of access location, such as administering antivirus, web filtering, VPN, and signature updates
- Administering FortiClient endpoint registrations, such as accepting, deregistering, and blocking registrations
- Managing endpoints, including status, system, and signature information
- Identifying outdated versions of FortiClient software

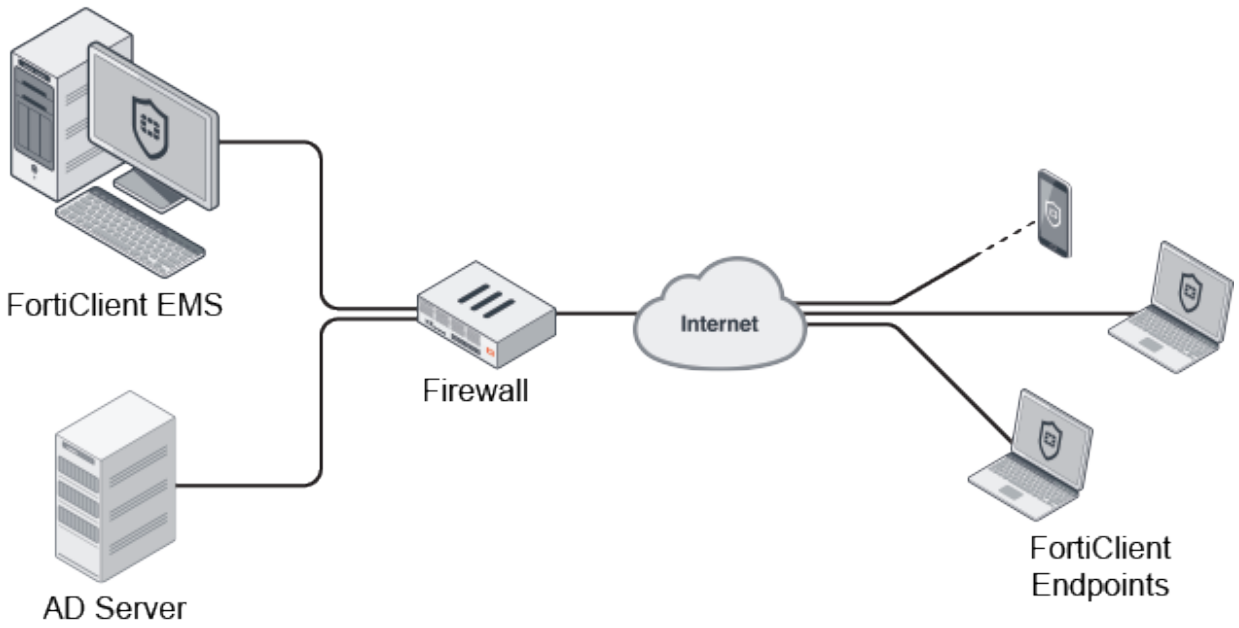
You can manage endpoint security for both Windows and Mac OS X platforms by using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view.

Components of FortiClient EMS

FortiClient EMS provides the infrastructure to install and manage FortiClient software on endpoints. FortiClient protects endpoints from viruses, threats, and risks.

The following table lists the components of FortiClient EMS.

Component	Description
FortiClient EMS	Manages FortiClient on endpoints that connect to your network. It includes the following software: • The console software that manages security profiles and FortiClient on endpoints • The server software that provides secure communication to and from endpoints and the console
Database	Stores security profiles and events. The SQL database is installed as part of the FortiClient EMS installation.
FortiClient	Helps enforce security and protection on endpoints. It runs on servers, desktops, and portable computers you want to secure. See the *FortiClient Administration Guide* on docs.fortinet.com for more information.



FortiClient EMS allows you to:

- Establish and enforce security profiles
- Manage deployment, configuration, and updates
- Obtain a consolidated view of multiple security components across all endpoint clients in your network
- Perform integrated installation of security components and set profiles

An informative video introducing you to FortiClient EMS is available in the Fortinet Video Library.

FortiClient EMS and Fortinet Endpoint Security Management

FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

Documentation

You can access the FortiClient EMS documentation from the following link: docs.fortinet.com

The FortiClient EMS documentation set includes the following documents:

- *FortiClient EMS 1.2.0 Release Notes*

  This document describes new features and enhancements in FortiClient EMS for the release and lists any known issues and limitations. This document also defines supported platforms and the required minimum system requirements.
- *FortiClient EMS 1.2.0 QuickStart Guide*

This document describes how to install and begin working with the FortiClient EMS system. It provides instructions on installation, deployment, and also includes a high-level task flow for using the FortiClient EMS system.

- *FortiClient EMS 1.2.0 Administration Guide*
  This document describes how to set up FortiClient EMS and use it to manage FortiClient endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor the FortiClient endpoints.

What's New

The following is a list of new features and enhancements in FortiClient EMS 1.2.

FortiClient EMS 1.2.0

Customize FortiClient installer

FortiClient EMS can create a FortiClient installer with any of the following components:

- SFA: The Security Fabric Agent provides endpoint telemetry, host vulnerability scanning, and remediation. This component is always selected and cannot be deselected.
- SAA: Secure Access Architecture includes SSL VPN and IPSec VPN features. This component is selected by default.
- APT: Advanced Persistent Threat components provide integration with FortiSandbox detection.
- ASF: Additional Security Features includes antivirus, web filtering, application firewall, and single sign-on mobility agent.

See Software Manager on page 85.

FortiClient for Mac OS X Vulnerability Scan support

Vulnerability Scan and auto-patching feature is now supported in FortiClient for Mac OS X. See Endpoint Profiles on page 51.

One-time pull of existing FortiClient profile from FortiGate

FortiClient EMS now supports a one-time pull of an existing FortiClient profile from FortiGate. The EMS administrator can pull an existing FortiClient profile from a FortiGate and modify it before deploying to endpoints. See Importing FortiGate profiles on page 54.

Pre-login banner

The pre-login banner feature can be used to display a message on the login page for FortiClient EMS before the user logs in. Users must accept the banner message before they can log in. See Configuring the pre-login banner on page 102.

Deployment improvements

FortiClient EMS has improved the installer deployment functionality so that more real-time deployment information is visible on FortiClient EMS. The deployment technique has also been enhanced so it is more reliable and provides a better user experience. See Viewing endpoints on page 39.

Redesigned Endpoints pane

The *Endpoints* pane has been redesigned to be more user-friendly. You can clearly see the endpoint installer deployment, profile synchronization, FortiClient Telemetry connection, and compliance status. The device information is also better organized for easier access. See Viewing the Endpoints content pane on page 39.

Get Started

This section provides an overview of how to perform the following tasks after you install FortiClient EMS:

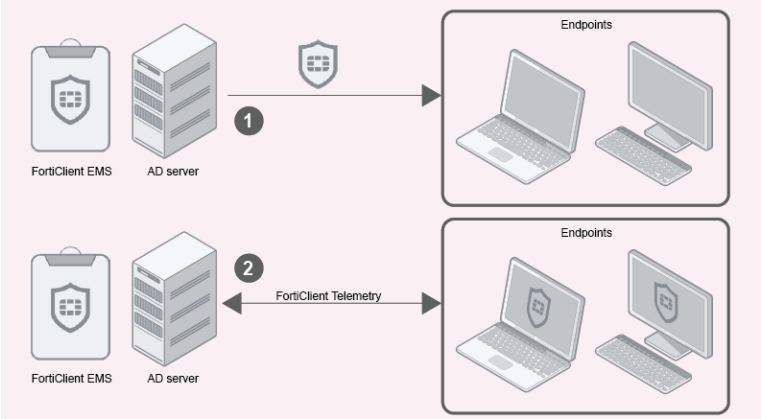
Deploying FortiClient software to endpoints

Following is an overview of how to add endpoints to FortiClient EMS and configure FortiClient EMS to deploy FortiClient to endpoints.

You can deploy FortiClient to endpoints by using AD servers and workgroups. There are differences between using AD servers and workgroups. You cannot use workgroups to deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

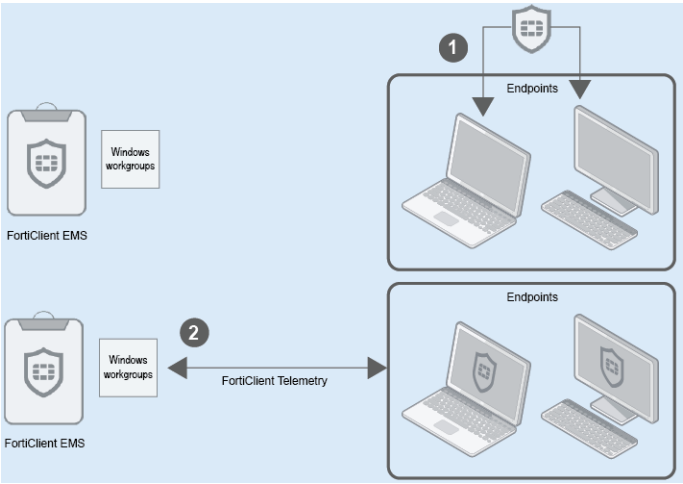
The image below shows a deployment of FortiClient using FortiClient EMS with an AD server:

1. Deploy FortiClient from FortiClient EMS using an AD server to the desired endpoints.
2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



The image below shows a deployment of FortiClient using FortiClient EMS with Windows workgroups:

1. Workgroups cannot be used with FortiClient EMS to initially install FortiClient on endpoint devices. FortiClient must be installed directly on endpoints. Endpoint users can access the Software Manager in FortiClient EMS to download and install FortiClient on endpoints. See Viewing installers in FortiClient Software Manager on page 88 for details.
2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



To deploy FortiClient software to endpoints:

1. Add endpoint devices by working with an AD service or Windows workgroups. See Adding endpoints on page 37.
   Endpoints added by using the AD service are displayed on the *Endpoints* > *Domain* pane, and endpoints added by using Windows workgroups are displayed on the *Endpoints* > *Workgroups* pane. You can install, upgrade, and uninstall FortiClient on endpoints using an AD server without registering FortiClient to FortiClient EMS as long as the username and password are correct on the profile's *Deployment* tab in FortiClient EMS. Note that workgroups can only be used to upgrade or uninstall FortiClient if it is already installed on the endpoints and registered to FortiClient EMS; workgroups cannot be used for initial installations of FortiClient. When using workgroups, the credentials on the *Deployment* tab in FortiClient EMS are not taken into account.
2. Add FortiClient installers to FortiClient EMS, and specify which FortiClient features each installer will install on endpoints. See Adding FortiClient installers on page 85.
3. Create a profile to select the FortiClient installer and include configuration information for FortiClient software on endpoints. See Creating profiles to deploy FortiClient on page 52.
4. Prepare domains and workgroups for deployment. See Preparing the AD server for deployment on page 81.
5. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles to endpoints on page 57.
   See also Deploying FortiClient on endpoint devices on page 83.

   After the profile is assigned to endpoints, its changes are pushed to endpoints. FortiClient is installed on endpoints, and FortiClient connects Telemetry to FortiClient EMS.
6. Monitor the installation process by using the Endpoints content pane. See Viewing the Endpoints content pane on page 39.

Pushing configuration information to FortiClient

After FortiClient software on endpoints has connected Telemetry to EMS, the endpoints are managed, and you can use FortiClient EMS to push configuration information to FortiClient software on endpoints.

To push configuration information to FortiClient:

1. Edit an existing profile or create a new profile to configure FortiClient software on endpoints. See Creating profiles to configure FortiClient on page 51.
2. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles to endpoints on page 57.

   After the profile is assigned to endpoints, its changes are pushed to endpoints with the next Telemetry communication.
3. Monitor the update by using the Endpoints content pane. See Viewing the Endpoints content pane on page 39.

Using EMS integrated with FortiGate

You can integrate FortiGate with FortiClient EMS. When used together, FortiGate is used for endpoint control and network access compliance (NAC), and FortiClient EMS is used to deploy and manage FortiClient software on endpoints.

When FortiGate is configured for NAC, you can use FortiOS to create a FortiClient profile that defines compliance rules and non-compliance action. The compliance rules define what configuration FortiClient software and the endpoint must have for the endpoint to maintain access to the network through FortiGate. The non-compliance action can either be *block* or *warn*, and it defines what action FortiGate takes when endpoints fail to comply with the compliance rules. When the non-compliance action is *block*, FortiGate blocks endpoints from accessing the network when they fail to comply with the compliance rules. When the non-compliance action is *warn*, FortiGate warns the endpoint about non-compliance, but allows network access after the endpoint user acknowledges the warning.

Although the compliance rules define what configuration FortiClient software and the endpoint must have, the FortiClient profile from FortiGate does not include any configuration information. The endpoint user or administrator is responsible for configuring the FortiClient console to adhere to the compliance rules. An administrator can use EMS to configure the FortiClient console.

After you create a FortiClient profile by using FortiOS, you can import the profile into FortiClient EMS, and edit the profile to add a FortiClient installer and specify configuration information for FortiClient software. Then you can use FortiClient EMS to deploy the updated profile containing both compliance rules and configuration information to endpoints.

To use EMS integrated with FortiGate:

1. Using FortiGate running FortiOS 5.6, create a FortiClient profile to define the compliance rules.
2. Using FortiClient EMS, import the FortiClient profile. See Importing FortiGate profiles on page 54.
3. Review the compliance rules.
4. Edit the imported profile to add configuration information that supports the compliance rules, and save the profile. You can add a FortiClient installer if needed.
5. Create a gateway IP list that includes the gateway IP address or fully qualified domain name (FQDN) for the FortiGate. See Creating gateway IP lists on page 78.

Each gateway IP list includes a list of one or more IP addresses or fully qualified domain names (FQDN) that FortiClient can use when registering to EMS or FortiGate.

6. Assign the gateway IP list to domains or workgroups as needed. See Assigning gateway IP lists to endpoints on page 80.

   FortiClient software uses the IP addresses in the gateway IP list to connect FortiClient Telemetry to EMS and/or FortiGate.

7. Assign the profile to domains or workgroups as needed. See Assigning profiles to endpoints on page 57.

   After the profile is assigned to endpoints, the compliance rules and settings are pushed to endpoints with the next Telemetry communication.

8. Use FortiClient EMS to monitor and manage endpoints. See Viewing the Endpoints content pane on page 39.
9. Use FortiClient EMS to update the profile as needed.

Installation Preparation

This section helps you prepare to install FortiClient EMS. Before you install FortiClient EMS, you should be aware of the following information:

Before installing FortiClient EMS, it is recommended that you read the *FortiClient EMS Release Notes* available on docs.fortinet.com to become familiar with relevant software components and other important information about the product.

Licenses

This section describes the licensing options available for FortiClient EMS. It provides information about the number of supported FortiClient endpoints for each type of license to help you determine which license best suits your needs.

FortiClient EMS

FortiClient EMS supports the following types of licenses:

- Free trial license
- Purchased license

Free trial license

When you install FortiClient EMS, the free trial license is enabled by default. The free trial license supports ten FortiClient endpoints. FortiClient EMS consumes one license count for each managed FortiClient device.

Purchased license

Each purchased license allows management of one FortiClient endpoint. You must purchase a minimum of 100 endpoints, and you have an option to have this EMS license for a maximum three year term. You can specify the number of endpoints and the duration of the term at the time of purchase.

You can use a licensed FortiClient EMS to deploy, provision, and manage FortiClient endpoints. However, if you have a FortiGate in your network, you can buy an add-on FortiGate endpoint license to enforce endpoint compliance on the firewall while end-points are being managed by EMS. Using FortiGate with EMS is optional.

An email will be sent when you are running out of licenses. Additionally, a log entry will be entered when a client is refused connection due to unavailable licenses.

Component applications

Common services or applications do not require a license.

During the installation of common services required for FortiClient EMS, you are not asked for license information.

Required services and ports

You must ensure that required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable ports 8013 and 10443 as these are opened by the FortiClient EMS installation.

Communication	Service	Protocol	Port
FortiClient endpoint/FortiClient Telemetry	File transfers	TCP	8013 (default)
Computer browser service • Allows FortiClient endpoints to automatically register to EMS. Computer browser service is not needed if an Active Directory is used or endpoint users can manually register FortiClient to EMS.	Enabled		
Samba (SMB) service • FortiClient EMS uses the SMB service during FortiClient deployment.	Enabled		445
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) • The FortiClient EMS server connects to the endpoints using RPC for FortiClient deployment.	Enabled		135
Active Directory server connection	When used as a default con-nection		389 (LDAP) or 636 (LDAPS)
FortiClient download	Enabled		10443 (default)
Apache	HTTPS	TCP	443

Communication	Service	Protocol	Port
SQL server			

Ensure that the Computer Browser Service is running. On Windows Server 2012 R2, the service is disabled by default. If this service is not active, FortiClient EMS cannot detect computers on the same network, even if they are available.

Management capacity

FortiClient EMS is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested host system hardware configurations for FortiClient EMS. The suggested configurations depend on the number of endpoints being managed by FortiClient EMS.

You will need at least **200GB** of free disk space available.

Max number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
10000	2	8	default
20000	4	8	default
30000	4	8	120 seconds
40000	4	8	120 seconds
50000	4	8	120 seconds
Suggested minimum system hardware for FortiClient EMS:			
75000	8	16	120 seconds

For the purpose of this table, an Intel i5 processor with two cores and two threads per core will be considered to have four virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

Server readiness checklist for installation

Use the following checklist to prepare your server for installation.

Checklist	Readiness Factor
	Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS. Installation might be slow or disrupted while these programs are active. Note that a server might be vulnerable to attack when you uninstall or disable security applications.
	Carefully consider the date and time settings that you apply to your server.
	Confirm that required services and ports are enabled and available for use by FortiClient EMS.
	Ensure that no conflict exists with port 443 for the Apache service to function properly.
	Ensure that no conflict exists with port 8013 for the EMS service to function properly.

Upgrading from an earlier version of FortiClient EMS

FortiClient EMS 1.2.0 supports upgrading from EMS 1.0.3 and later 1.0 versions. To ensure a successful upgrade, it is recommended you perform the upgrade on a staging server before upgrading the production server. Follow the procedure below.

1. (Optional) Back up the database from the EMS 1.0.x production server.
2. Install EMS 1.0.x on a staging server.
3. (Optional) Import the EMS 1.0.x database from the production server.
4. Register FortiClient endpoints to the staging server.
5. Upgrade the staging server to EMS 1.2.0.
6. Monitor the staging server for two days.
7. Upgrade the production server to EMS 1.2.0.

Installation and Licensing

Before you install and license FortiClient EMS on a server, ensure you have:

- Reviewed Licenses on page 1
- Met the requirements listed in the Required services and ports on page 18
- Completed the Server readiness checklist for installation on page 19
- Logged into the server as the administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS, and other application tasks. You can use this account to initially log into the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended that you install FortiClient EMS on a dedicated server in a controlled environment. Installing other software applications can interfere with the normal operation of FortiClient EMS.

Downloading the installation file

FortiClient EMS is available for download from the following location:

- Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS:

- `FortiClientEnterpriseManagement_1.2.0.<build>_x64.exe`

For more information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS

The FortiClient EMS installation package includes:

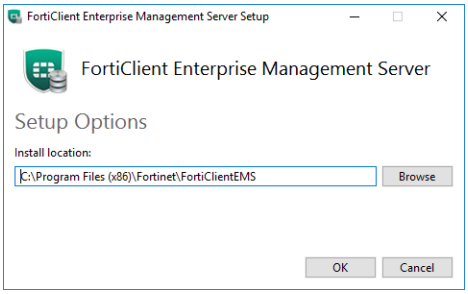
- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

Local administrator rights and Internet access are required to install FortiClient EMS.

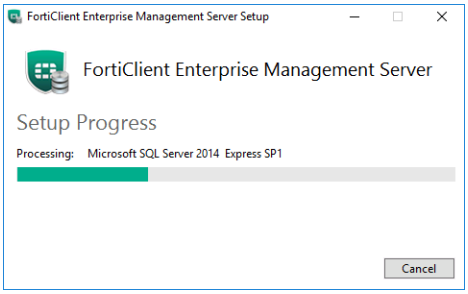
To install FortiClient EMS:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator* from the popup menu.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions*, if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

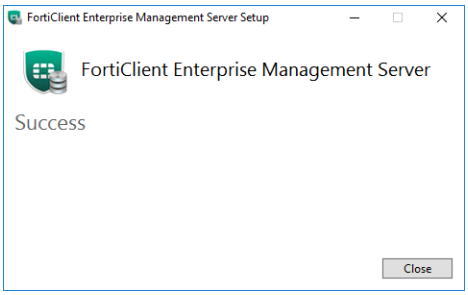
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.



   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.
5. Click *Install*.
   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others. Please be patient.



6. When the program has installed correctly, the *Success* window will be displayed. Click *Close* to close the window.



A *FortiClient Enterprise Management Server* icon will be added to the desktop.

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon to start FortiClient EMS.
2. Sign in with username *admin* and no password.
3. Change the username and password by going to *View* > *User Management* > *Administration*.
4. Configure FortiClient EMS by going to *View* > *Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely by using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *View* > *Settings*.
2. On the *Server Settings* tab, enable *Remote Administration HTTPS Access*.
3. In the *Custom Host Name* box, type the host name or IP address.
4. Click *Save*.

To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure that you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or by adding it to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Licensing FortiClient EMS

An instructional video on how to obtain licensing for FortiClient EMS is available in the Fortinet Video Library.

To license FortiClient EMS:

1. Purchase FortiClient EMS from a reseller.

   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS, you will receive the *FortiClient Host Security License Certificate* via email. This email contains the *Certificate Number* that will be used to obtain the FortiClient EMS License.

2. Log into the Fortinet Support site.
3. Register FortiClient EMS:
   a. Click *Register and Renew*.
   b. Enter the *Certificate Number*. This is the number you received in the FortiClient Host Security License Certificate email.

      If you have not already registered an EMS device, you will be prompted to do so. This will require obtaining the *Hardware ID* from FortiClient EMS. You can obtain the *Hardware ID* by going to *Help > About > Hardware ID*.

   c. Enter the *Hardware ID*.
   d. Enter the *Fortinet Partner Reseller*.
   e. Read, verify and agree to the *Terms and Conditions* of the service.
   f. Verify the Product Entitlement List for your recent FortiClient EMS purchase. Check the *By accepting these terms...* checkbox. Then, click *Confirm*. The license file will now be available to use with your FortiClient EMS installation.
   g. Click *Finish*.
4. Retrieve the license key:
   a. From your *Products List*, select FortiClient EMS.
   b. From the left panel, select *License and Key*.
   c. From the *Available Keys List*, select the FortiClient EMS entry. Then, click *Get the License File*.
5. License FortiClient EMS:
   a. From FortiClient EMS, go to *View > Upgrade License*, and click *Browse*.
   b. Select the license file and click *Upload File*. You have successfully licensed FortiClient EMS.

If you need to upgrade or renew your license, please contact Fortinet Support.

License status

The status of your license is displayed in the *Dashboard > System Information* widget. The status of your license can change. The options are:

License Status	Description
Trial	If you have just installed FortiClient EMS, the trial license is enabled by default. You should upload the license file that you purchased.

License Status	Description
Non-Expired License	You have the option to upgrade the license. For more information, see License upgrades or renewals on page 95.
Expired License	You have the option to renew the license. For more information, see License upgrades or renewals on page 95.

Help with licensing

For licensing issues with FortiClient EMS, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

Specifying different ports

In cases where there are pre-existing services running on default FortiClient EMS ports, you can specify another port by using the CLI to run the installer. You can use the following commands:

Command	Description
`ClientDownloadPort`	The port FortiClient will be downloaded from FortiClient EMS.
`RemoteManagementPort`	The port that will be used for EMS administration.

Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise

FortiClient EMS is installed with Microsoft SQL Server Express. This has a file size limit of 10 GB per database. Log entries recorded in the database are rotated on a schedule of seven days (one week) by default. If the FortiClient deployment is large, the database size may reach the 10 GB limit over time. The EMS admin may upgrade the SQL Server from Express to Standard or Enterprise edition. The database file size limit for both of these two editions is in the PB range (unlimited for most practical usage).

Microsoft SQL Server Express is a free edition. All other editions require a license from Microsoft.

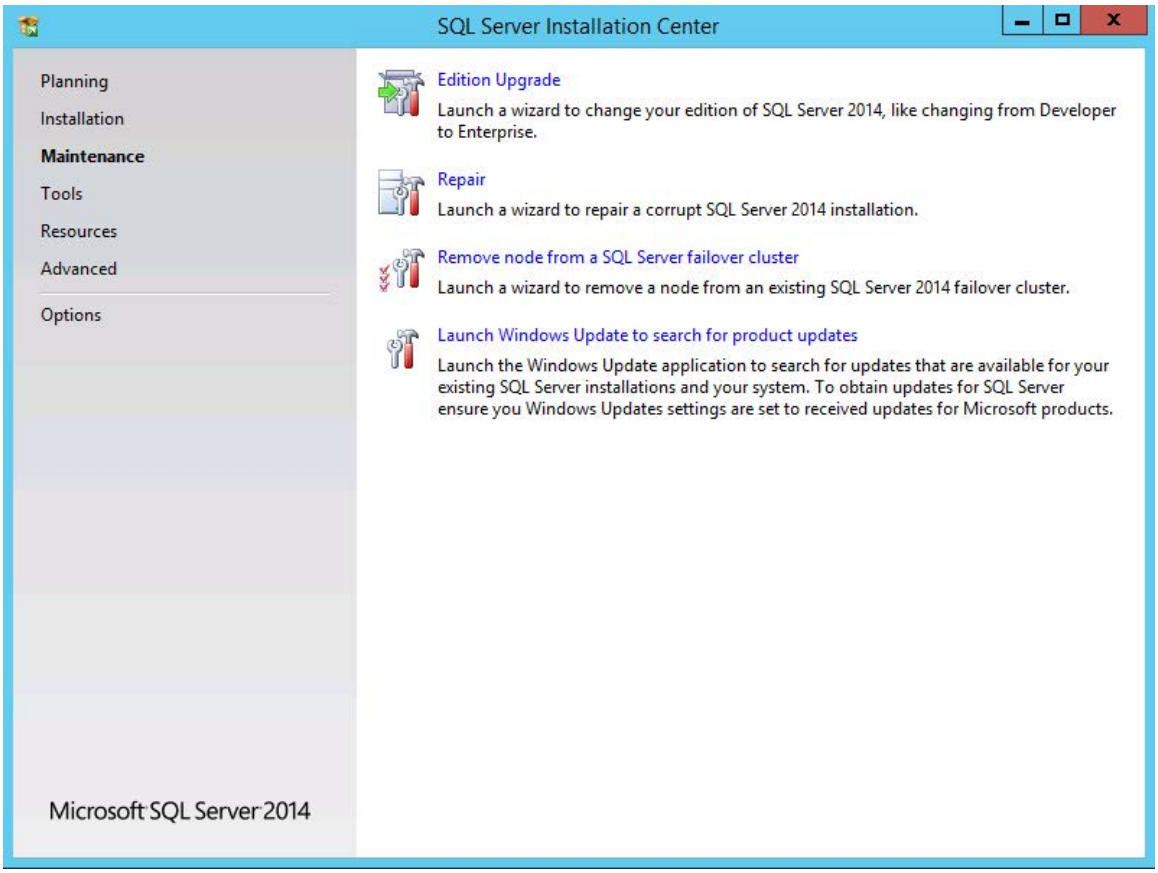
See also the following Microsoft documentation on upgrading between editions called *Upgrade to a Different Edition of SQL Server 2014 (Setup)* located at https://technet.microsoft.com/en-us/library/cc707783(v=sql.120).aspx

The EMS database is saved in the *C:\Program Files\Microsoft SQL Server\MSSQL12.FCEMS\MSSQL\DATA\FCM_root.mdf* file in the EMS host server. The size of this file should remain below the 10 GB limit for Microsoft SQL Server Express.

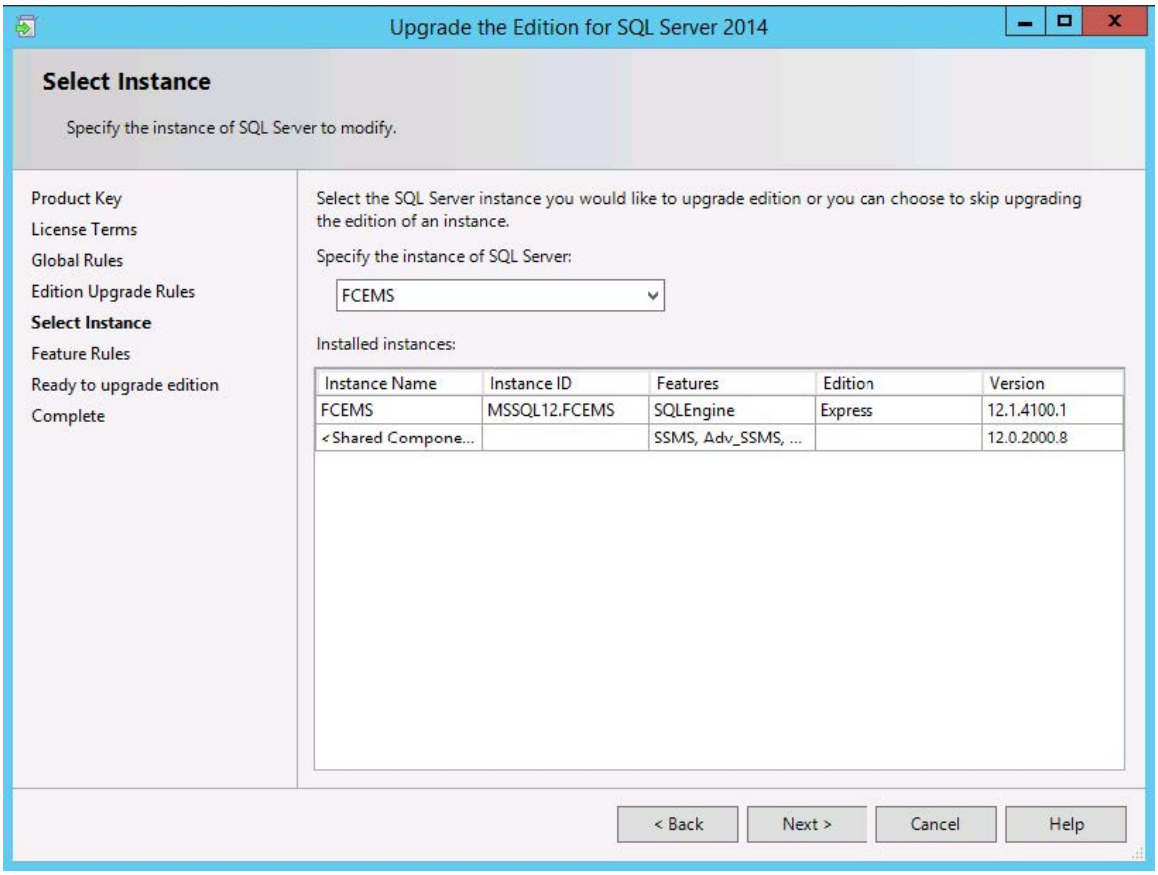
It is recommended to do a database edition upgrade outside normal production hours.

To upgrade Microsoft SQL Server Express:

1. Attach the SQL Server 2014 installation media to the EMS server.
   The installation media is a DVD or ISO file. If you are using the DVD, insert the DVD into the EMS host computer (host server). Use the ISO file if your host server is a virtual machine.
2. Run the SQL Server setup application wizard.
3. In the SQL Server Installation Center wizard, go to *Maintenance* > *Edition Upgrade*.



4. Enter the *product key*.
5. Accept the license terms. Then, click *Next*.
6. Under *Select Instance*, in the *Specify the instance of SQL Server* dropdown list, select *FCEMS*. Then, click *Next*.



7. Under *Ready to upgrade edition*, click *Upgrade*.
8. After the upgrade is complete, click *Finish*.

Testing the SQL server upgrade

It is recommended to run a short test on FortiClient EMS after the upgrade to verify proper operations. A simple test may be to:

- Register FortiClient on one or two test endpoints to EMS.
- Create a new custom group in FortiClient EMS and add the test endpoints to the new custom group.
- Create a new endpoint profile, and assign it to the new custom group.
- Check that FortiClient on the test endpoints received the new profile.

Monitor the system closely over the first few days for any unusual behavior.

Uninstalling FortiClient EMS

Use the *Programs and Features* pane of the Control Panel in Microsoft Windows to uninstall FortiClient EMS.

FortiClient EMS installs the following dependencies. If they are not being used by other applications on the same computer, they can be uninstalled manually after the EMS has been removed.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

To uninstall FortiClient EMS:

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

GUI

The FortiClient EMS GUI consists of the following areas:

- Banner
- Left pane
- Content pane

Banner

Option	Description
License Information	Displays current license status and number of licenses.
Envelope Icon	Click the Envelope icon to display all alert logs.
View	View and configure the following: • Upgrade License • Software Manager • User Management • CA Certificate Management • Database Management • View Logs • Settings
Help	View the following: • Technical Documentation • How-To Videos • Forums • Getting Started • Create Support Package • About
<Logged in user name>	Click the dropdown list beside the <logged in user name> to log out of FortiClient EMS.

Left pane

The left navigation pane is used to display content in the right content pane.

Option	Description
Dashboard	Displays a dashboard of information about all managed endpoints.
Vulnerability Scan	Displays the Vulnerability Scan Summary Chart that provides a centralized vulnerability summary for all monitored endpoints. You can observe high-risk hosts and critical vulnerabilities existing on endpoints. You can also access links on how to fix or repair the vulnerabilities.
Endpoints	Add and manage endpoints. You can add and manage endpoints from domains and from workgroups.
Endpoint Profiles	Create and assign profiles as well as manage profile updates.
Gateway IP Lists	Create and assign gateway IP lists as well as manage IP list updates.

Content pane

The right content pane displays the user interface controls that correspond to the selection you make in the left pane. The status and menu icons in the top-right display controls what you can use to configure additional settings for user management and each individual endpoint.

Dashboard

You can use the dashboard to view summary information about the system and endpoints. You can also view summary information about vulnerability scans on endpoints.

Viewing the Dashboard

To view the Dashboard:

1. In the left pane, click *Dashboard*.
   A *System Information* widget as well as charts and widgets of summary information are displayed. For descriptions, see System Information widget on page 31 and Dashboard charts and widgets on page 32.
2. Click an event summary.
   The list of endpoints for the summary is displayed.
3. Click the *Back* button to return to the *Dashboard*.
4. Click a pie chart.
   The *Endpoints* content pane is displayed with more details about the endpoints related to the pie charts. See also Viewing the Endpoints content pane on page 39.

System Information widget

The following information is displayed in the *System Information* widget:

Option	Description
Hostname	Name of the computer on which FortiClient EMS is installed.
Serial Number	Serial number for FortiClient EMS.
License Status	Status of the license for FortiClient EMS. See also Licensing FortiClient EMS on page 23.
Used Licenses	Number of used licenses out of the total number of available licenses. Also displays a button for entering, upgrading, and renewing a license, depending on the license status. If you have just installed EMS, click the *Enter License* button to upload your license file. If you have a non-expired license, but would like to upgrade your license, click the *Upgrade* button to upgrade your license file. If your current license is expiring, the *Renew* button will be enabled for you to upload your new license file.
System Time	Time and date used by the computer on which FortiClient EMS is installed.

Option	Description
System Database	Options to back up and restore the database. Click *Backup* to back up the database. Click *Restore* to restore a backed up database.
Current Admin	Name of the administrator logged into FortiClient EMS.
Uptime	Number of days, hours, minutes, and seconds that FortiClient EMS has been running.

Dashboard charts and widgets

The Dashboard displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each of the charts are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Client Stats	Statistics of clients in use. The data in this widget is determined by the value entered in the *Settings* > *Log Settings* > *Auto Remove Web Filter Logs* section. • Managed and Unmanaged • Online and Offline • On-Net and Off-Net
FortiGate Managed Endpoints Summary Chart	This chart indicates how many clients are unregistered and registered to which FortiGates. It provides an overview of the FortiGate Managed Endpoint status.
Devices by Windows Version	This chart indicates the number of endpoints running each version of a Windows operating system.
Devices by Mac Version	This chart indicates the number of endpoints running each version of a Mac operating system.
Event Summary	Summary of events: • Endpoints with Out-of-date Protection • Endpoints with Out-of-sync Profiles • Endpoints with Pending Software Updates • Errors or Warnings (last <number> days) • Inactive Endpoints (last <number> days) • Unprotected Clients
Installed FortiClient Version Summary - Windows	This chart indicates the percentage of endpoints with each version of FortiClient (Windows) installed.
Installed FortiClient Version Summary - Mac	This chart indicates the percentage of endpoints with each version of FortiClient (OS X) installed.

Viewing the Vulnerability Scan Dashboard

To view the Vulnerability Scan dashboard:

1. In the left pane, click *Vulnerability Scan*. Charts and widgets display a summary of vulnerability scan information.
2. Click any of the pie charts to view more details about the vulnerabilities.

Vulnerability scan charts and widgets

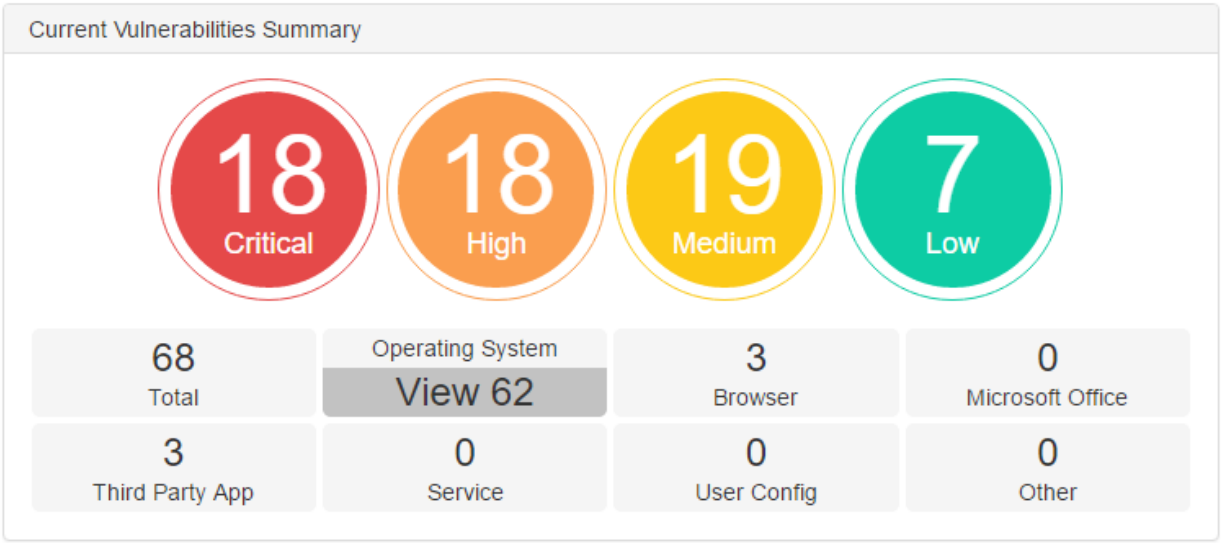
The *Vulnerability Scan Dashboard* displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each of the charts are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Current Vulnerabilities Summary	Displays the following summaries of current vulnerabilities: • Total (total number of the vulnerabilities) • Operating System (number of operating system vulnerabilities) • Browser (number of browser vulnerabilities) • Microsoft Office (number of Microsoft Office vulnerabilities) • Third Party App (number of third party application vulnerabilities) • Service (number of service vulnerabilities) • User Config (number of user configuration vulnerabilities) • Other (number of other vulnerabilities that do not fit any of the above categories) When you click on a vulnerability tile, the severity of vulnerabilities will be displayed in the colored circles above.
Host Scan Summary	Displays the following summaries about hosts: • Vulnerable Hosts • Un-Scanned Hosts • Secured Hosts • Scanning Hosts
Top 10 Vulnerable Hosts	Displays the Top 10 Vulnerable Hosts and the number of vulnerabilities within that host.
Top 10 Vulnerabilities	Displays the Top 10 Vulnerabilities.

Viewing current vulnerabilities

To view current vulnerabilities:

1. Click a *Vulnerability Tile*.
2. The colored circles change and display the number of vulnerabilities and severities corresponding to the selected *Vulnerability Tile*.



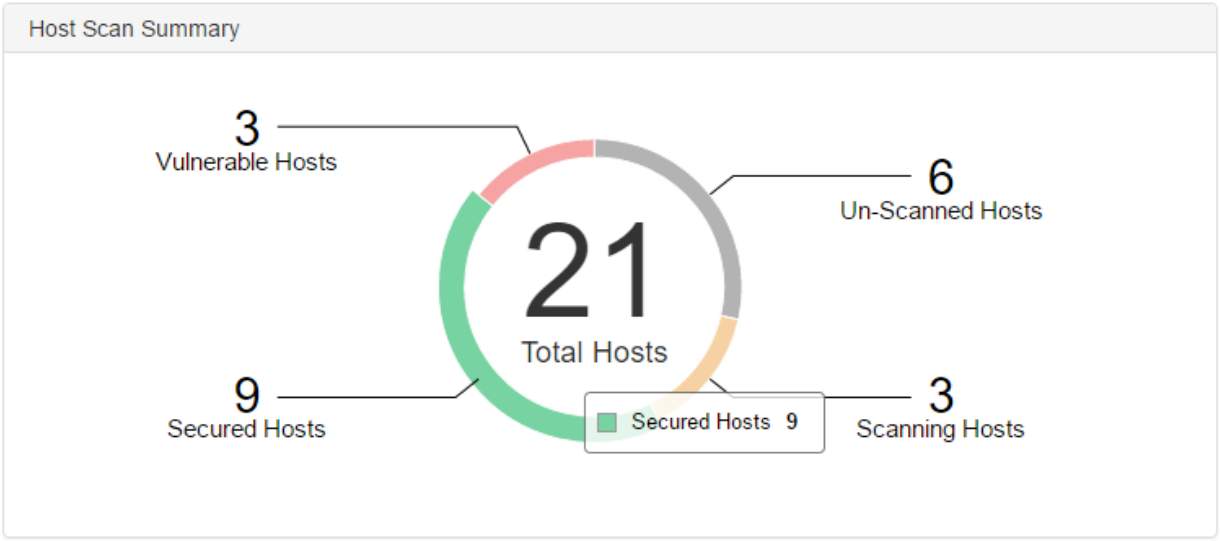
For example, click the *Operating System* tile, which has a total of 62 *Vulnerabilities*. The *Vulnerabilities* are organized by *Severity*:

- 18/62 are *Critical* (red circle)
- 18/62 are *High Risk* (orange circle)
- 19/62 are *Medium Risk* (yellow circle)
- 7/62 are *Low Risk* (green circle).

Viewing the Host Scan Summary

To view the Host Scan Summary:

1. Click a section of the *Host Scan Summary Donut* chart.
   The Endpoint content pane is displayed with information about the hosts corresponding to the section.

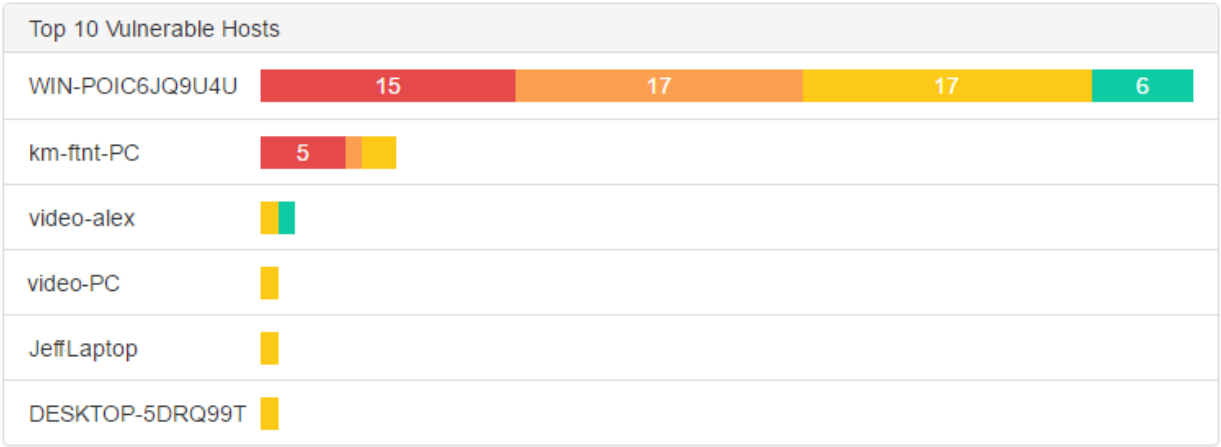


For example, click the *Secured Hosts* section, which has a total of 21 hosts. The hosts are organized by type:

- 9/21 are *Secured Hosts* (green section)
- 3/21 are *Vulnerable Hosts* (red section)
- 6/21 are *Un-Scanned Hosts* (yellow section)
- 3/21 are *Scanning Hosts* (grey section)

Viewing the top 10 vulnerabilities on hosts

How to read the Top 10 Vulnerable Hosts widget:



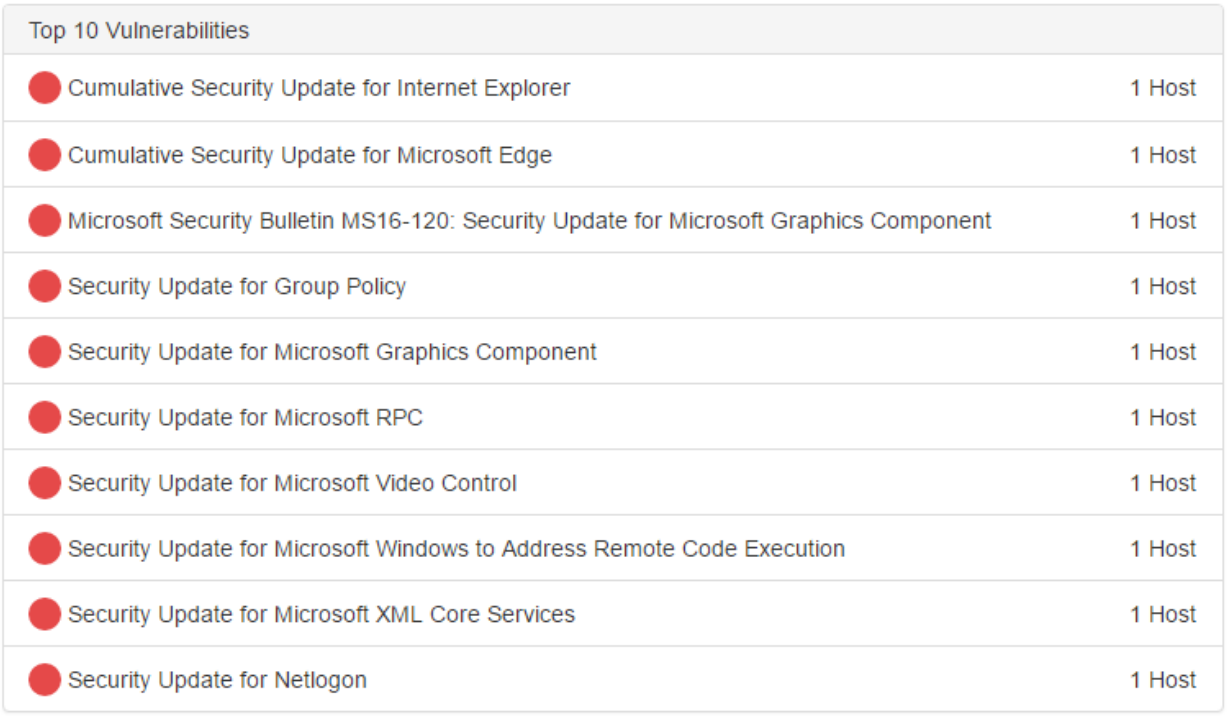
For example, the *Top 10 Vulnerable Hosts* vulnerabilities are displayed. The *Vulnerabilities* are shown in a segmented bar graph and organized by severity:

WIN-POIC6JQ9U4U has the following:

- 15 *Critical Vulnerabilities* (red bar)
- 17 *High Risk Vulnerabilities* (orange bar)

- 17 *Medium Risk Vulnerabilities* (yellow bar)
- 6 *Low Risk Vulnerabilities* (green bar)

How to read the Top 10 Vulnerabilities widget:



The *Top 10 Vulnerabilities* widget displays the type of vulnerability and how many hosts have the vulnerability. For example, the *Cumulative Security Update for Internet Explorer* vulnerability has one host affected.

When you click on a vulnerability, you will be redirected to the *FortiGuard Encyclopedia Vulnerability Center* where more details about the vulnerabilty are available.

Endpoints

FortiClient EMS needs to determine which devices to manage. Device information can come from an Active Directory service, Windows workgroup, or manual FortiClient registration. You can also create groups to organize endpoints.

Creating groups

You can create groups to organize endpoints. You can also rename and delete groups.

To create groups:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Create Group*. The *Group Name* dialog box is displayed.
3. In the *Please provide a group name* box, type a name for the group, and click *OK*.
   The group is created.

To rename groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Rename Group*. The *Group Name* dialog box is displayed.
3. In the *Please provide a group name* box, type the new name, and click *OK*.
   The group is renamed.

To delete groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Delete Group*. A confirmation dialog box is displayed.
3. Click *Yes*.
   The group and any subgroups are deleted.

Adding endpoints

You can add endpoints by using an Active Directory service. Endpoints are also added when endpoint users manually connect FortiClient Telemetry to FortiClient EMS.

Adding endpoints using an Active Directory domain service

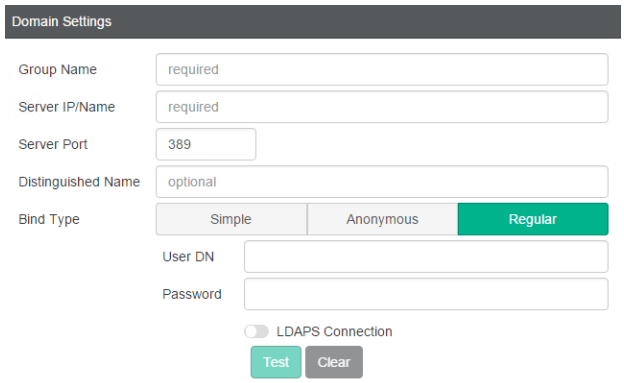
Endpoints can be manually imported from an Active Directory (AD) domain service. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying the endpoint devices that are part of an Active Directory (AD) domain service.

An instructional video on how to add a domain is available in the Fortinet Video Library.

You have the option to add the entire domain or just an organizational unit (OU) from the domain.

To add endpoints using an Active Directory domain service:

1. Click *Endpoints* > *Add a New Domain*. The *Domain Settings* pane is displayed.



2. Configure the following options:

Group Name	Enter a name for the group. The name will be displayed in the FortiClient EMS Endpoint view
Server IP/ Name	Type the IP address or name.
Server Port	Type the port number.
Distinguished Name	Type the distinguished name (optional).
Bind Type	Select the bind type. *Simple*, *Anonymous*, *Regular* . When you select *Regular*, enter the *User DN* and *password*.
User DN	Available when *Bind Type* is set to *Regular*. Type the user DN.
Password	Available when *Bind Type* is set to *Regular*. Type the user password.
Show Password	Available when *Bind Type* is set to *Regular*. Turn on and off to show or hide the password.
LDAPS	Turn on to enable a secure connection protocol when *Bind type* is set to *Regular*.

3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required then test the settings again.

Connecting manually from FortiClient

Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient console. This process is sometimes called registering FortiClient to FortiClient

EMS.

To connect FortiClient Telemetry to FortiClient EMS:

1. In FortiClient console on the endpoint device, go to the *Compliance* tab.
2. In the *FortiGate or EMS* box, type the IP address for EMS, and click *Connect*.
   FortiClient registers to FortiClient EMS.

For more information about FortiClient, see the *FortiClient Administration Guide* available on the docs.fortinet.com site.

The FortiClient Telemetry gateway port may be appended to the gateway IP list address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to register to the IP address given by using the default port. The default registration port in FortiClient 5.2 is 8010 and in FortiClient 5.4 is 8013. FortiClient EMS listens for registration on port 8013 by default.

Viewing endpoints

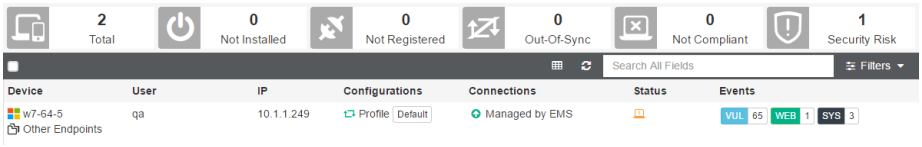
After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup in the *Endpoints* pane. You can also view details about each endpoint in the *Client Details* pane and use filters to access endpoints with specific qualities.

Viewing the Endpoints content pane

You can view information about endpoints on the *Endpoints* content pane.

To view the Endpoints content pane:

1. Go to *Endpoints*, and select a domain or workgroup.
   The list of endpoints in FortiClient EMS is displayed in the content pane as well as a quick status bar and a toolbar.



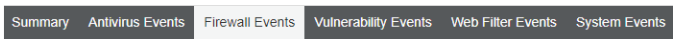
Total	Number of endpoints. Click to display the list.
Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints that are not registered to either FortiClient EMS or FortiGate. Click to display the list of unregistered endpoints.
Out of Sync	Number of endpoints that have an out of sync profile. Click to display the list of endpoints with out of sync profiles.

Not Compliant	Number of endpoints not compliant with the FortiGate compliance rules. Click to display the list of not compliant endpoints.
Security Risk	Number of endpoints that are a security risk. Click to display the list of endpoints.
Checkbox	Click to select all endpoints that are displayed in the content pane.
Show/Hide Heading	Click to hide and display the following column headings: *Device*, *User*, *IP*, *Configurations*, *Connections*, *Status*, and *Events*.
Refresh	Click to refresh the list of endpoints in the content pane.
Search box	Type a value and press *Enter* to search for the value in the list of endpoints.
Filters	Click to display and hide the filters that you can use to filter the list of endpoints for the selected domain or workgroup.
Device	Visible when headings are displayed. Displays an icon to represent the operating system on the endpoint as well as the name of the device.
User	Visible when headings are displayed. Displays the name of the user logged into the endpoint.
IP	Visible when headings are displayed. Displays the IP address for the endpoint.
Configurations	Visible when headings are displayed. Displays the name of the profile assigned to the endpoint and the synchronization status of the profile.
Connections	Visible when headings are displayed. Displays whether the endpoint is connected to FortiClient EMS or FortiGate and the connection status of *Online*, *Offline*, or *Not Registered*.
Status	Visible when headings are displayed. Displays one of the following compliance statuses for the endpoint. • Compliant • Not compliant • Not participating in compliance • Quarantined • Excluded • Not registered • Not installed
Events	Visible when headings are displayed. Displays FortiClient events for the endpoint.

2. Click an endpoint to display more details about it in the content pane.
   The following dropdown lists are displayed in the toolbar for the selected endpoint:

Checkbox	Click to select and deselect all endpoints in the content pane. You can then select or clear the checkbox for individual endpoints to fine tune the list of selected endpoints.
Scan	Click to start a Vulnerability or AntiVirus scan on the selected endpoint.
Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Action	Click to perform one of the following actions on the selected endpoint: • Upload FortiClient Logs • Request Diagnostic Results • Update Signatures • Re-register • De-register • Register • Quarantine • Un-quarantine • Exclude from Management • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint:



Summary		
	<user name>	Displays the name of the user logged into the selected endpoint.
	Device	Displays the device name for the selected endpoint.
	OS	Displays the operating system and version for the selected endpoint.
	IP	Displays the IP address for the selected endpoint.
	MAC	Displays the MAC address for the selected endpoint.
	Last Seen	Displayed the last date and time that FortiClient sent a keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive message occurred.
	Location	Displays whether the selected endpoint is onnet or offnet.

	Connection	Displays when the selected endpoint is connected to FortiClient EMS or FortiGate. Also displays the status of the connection.
	Configuration	Displays the following information for the selected endpoint: • Profile: Name of the profile assigned to the selected endpoint • Installer: Name of the FortiClient installer used for the selected endpoint. Displays *Not Assigned* if no FortiClient installer has been assigned to the selected endpoint. • IP List: Name of the gateway IP list used for the selected endpoint. Displays *Not Assigned* if no gateway IP list has been assigned to the selected endpoint. • FortiClient Version: Version of FortiClient installed on the selected endpoint.
	Compliance	Displays if the endpoint is compliant. If the endpoint is not compliant, displays the features for which FortiClient is not compliant.
	Features	Displays which features are enabled for FortiClient.
Antivirus Events		
	Date/Time	Displays the date and time of the antivirus event.
	Message	Displays the message for the antivirus event.
Firewall Events		
	Date/Time	Displays the date and time of the firewall event.
	Message	Displays the message for the firewall event.
Vulnerability Events		
	Vulnerability	Displays the name of the vulnerability. For example, *Security update available for Adobe Reader*.
	Category	Displays the vulnerability's category. For example, *Third Party App*.
	Application	Displays the name of the application with the vulnerability.
	Severity	Displays the severity of the vulnerability.
	FortiGuard ID	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it will redirect you to FortiGuard where further information will be provided if available.
	Bulletin	Displays a link to a bulletin about the software vulnerability.
Web Filter Events		

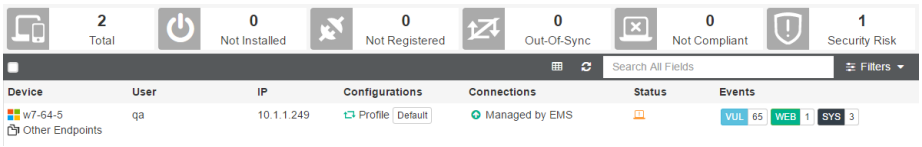
	Date/Time	Displays the date and time of the web filter event.
	Message	Displays the message for the web filter event.
System Events		
	Date/Time	Displays the date and time of the system event.
	Message	Displays the message for the system event.

Using the quick status bar

You can use the quick status bar to quickly display filtered lists of endpoints on the *Endpoints* content pane.

To use the quick status bar:

1. Go to *Endpoints*.
2. Click a domain or workgroup.
   The list of endpoints and the quick status bar are displayed.



3. Click one of the following buttons in the quick status bar:
   - Total
   - Not Installed
   - Not Registered
   - Out-Of-Sync
   - Not Compliant
   - Security Risk

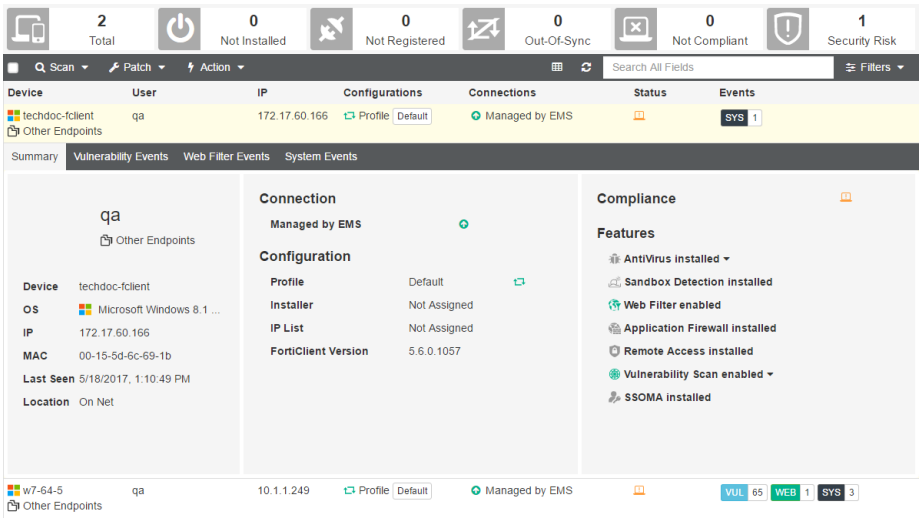
   The list of affected endpoints is displayed.
4. Click an endpoint to display details about the endpoint.
5. In the *Events* column, click the *Vul<number>*, *Web <number>*, *SYS<number>*, *AV<number>*, and *FW<number>* buttons to display the associated tab of details for the selected endpont.
6. Click the *Total* button to clear the filters.
   The unfiltered list of endpoints is displayed.

Viewing endpoint details

You can view each endpoint's detailson the *Endpoints* content pane. For a description of the options on the *Endpoints* content pane, see Viewing the Endpoints content pane on page 39.

To view endpoint details:

1. Go to *Endpoints*, and select a domain or workgroup.
   The list of endpoints for the selected domain or workgroup is displayed.
2. Click an endpoint to display more details about it in the content pane.
   Details about the endpoint are displayed in the content pane.



Filtering the list of endpoints

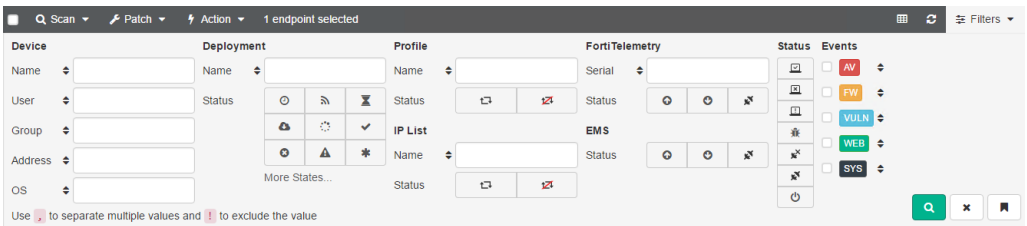
You can filter the list of endpoints displayed on the *Endpoints* content pane.

To filter endpoints:

1. Go to *Endpoints*.
2. Click a domain or workgroup.
   The list of endpoints is displayed.
3. Click the *Filters* menu, and set filters.
   The filter options are displayed.

   For text values, you can use a comma (,) to separate values, and you can use an exclamation mark (!) to exclude a value.

   For buttons, hover the mouse over each button to view its tooltip.



Device		Lists the filter options for devices.
	Name	Type the name or names to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	User	Type the name of the user or users to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Group	Type the name of the group or groups to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Address	Type the IP address to include in the filter. You can also exclude an IP address from the filter by using an exclamation mark (!).
	OS	Type the name of the operating system(s) to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
Deployment		Lists the filter options for deployment.
	Name	
	Status	Click one or more deployment status buttons to include in the filter. Selected status buttons are green. Hover the mouse over each button to view its tooltip. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
	More States	Click to display additional statuses to include in the filter.
Profile		
	Name	Type the name or names of the profile to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the profile status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-of-sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
IP List		
	Name	Type the name or names of the gateway IP list to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the gateway IP list status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-of-sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
FortiTelemetry		

	Serial	Select the serial number for the FortiGate to include in the filter.
	Status	Click the status for FortiClient Telemetry connection to FortiGate to include in the filter. Choose between *Online*, *Offline*, and *Not Registered*.
EMS		
	Status	Click the status for FortiClient Telemetry connect to EMS to include in the filter. Selected status buttons are green. Choose between *Online*, *Offline*, and *Not Registered*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Status		Click the status for compliance to include in the filter. Selected status buttons are green. Choose between *Compliant*, *Not Compliant*, *Not Participating*, *Quarantined*, *Excluded*, *Not Registered*, *Not Installed*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Events		Select the events to include in the filter. The selected check boxes beside the events are included in the filter. Clear the check box beside the event to exclude the event from the filter.
Bookmarks		Displays the list of saved filter settings. Displays only after you have saved a bookmark. Click the *Bookmark* button to name and save filter settings. Click a bookmark to use the saved settings. Click the *x* beside a bookmark to delete it.
Search		Click the *Search* button to apply the filter setting.
Reset		Click the *Reset* button to clear the filter settings.
Bookmark		Click the *Bookmark* button to save the filter settings as a bookmark.

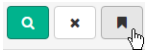
4. Click the *Search* button.
   The filtered list of endpoints is displayed.
5. Click the *Reset* button to clear the filter settings.

Using bookmarks to filter the list of endpoints

You can save filter settings as bookmarks, and then select the bookmarks to use them.

To create bookmarks to filter endpoints:

1. Go to *Endpoints*.
2. Click a domain or workgroup.
   The list of endpoints is displayed.
3. Click the *Filters* menu, and set filters.
4. Click the *Bookmark* button.



The *New Bookmark* box is displayed.

5. In the *New Bookmark* box, type a name for the filter settings, and press *Enter*.
   The bookmark is displayed under *Bookmarks*.

To use bookmarks to filter the list of endpoints:

1. Go to *Endpoints*.
2. Click a domain or workgroup.
   The list of endpoints is displayed.
3. Click the *Filters* menu.
4. In the *Bookmarks* list, click a bookmark.
   The bookmark settings are used to filter the list of endpoints.

Managing endpoints

You can manage endpoints from the *Endpoints* pane.

Running AntiVirus scans on endpoints

You can run a full or quick AntiVirus scan on endpoints.

To run AntiVirus scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Full AV Scan* or *Quick AV Scan*.
   Scanning starts on the endpoints with the next FortiClient Telemetry communication.

Running vulnerability scans on endpoints

You can run a vulnerability scan on endpoints. You can view the history of vulnerability scans for each endpoint on the *Client Details* pane.

To run vulnerability scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Vulnerability Scan*.
   Vulnerability scanning starts on the endpoints with the next FortiClient Telemetry communication.

To run vulnerability scans on an endpoint:

1. Go to *Endpoints*.
2. Select a domain or workgroup.
   The list of endpoints is displayed in the content pane.

3. Click an endpoint, and from the *Scan* menu, select *Vulnerability Scan*.
   Vulnerability scanning starts on the endpoint with the next FortiClient Telemetry communication.

Patching vulnerabilities on endpoints

You can request that FortiClient patch detected critical and high vulnerabilities on endpoints.

FortiClient can automatically patch many software. However, some detected software vulnerabilities must be manually patched by the endpoint user. If a vulnerability requires the endpoint user to download and install software to patch a vulnerability, the FortiClient console displays the information.

To patch vulnerabilities on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Patch Critical and High Vulnerabilities*.
   FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

To patch vulnerabilities on an endpoint:

1. Go to *Endpoints*.
2. Select a domain or workgroup.
   The list of endpoints is displayed in the content pane.
3. Click an endpoint, and from the *Patch* menu, select one of the following options:
   - *Selected Vulnerabilities on Selected Clients*
   - *Selected Vulnerabilities on All Affected Clients*
   - *All Critical and High Vulnerabilities*

   FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

Uploading FortiClient logs

You can upload a FortiClient log file from one or several endpoints to EMS. The log file is uploaded to the hard drive on the computer on which you are running EMS. The uploaded log file is not visible in FortiClient EMS GUI.

To upload FortiClient logs:

1. Go to *Endpoints*.
2. Select a domain or workgroup.
   The list of endpoints is displayed in the content pane.
3. Click one or multiple endpoints, and from the *Action* menu, select *Upload FortiClient logs*.
   The `<number>_log` file is uploaded to the following location on your computer: `<drive>\Program Files (x86)\Fortinet\FortiClientEMS\logs`

Running the FortiClient Diagnostic Tool

You can use EMS to run the FortiClient Diagnostic Tool on one or multiple endpoints and export the results to the hard drive on computer on which you are running FortiClient EMS. The exported information is not visible in FortiClient EMS GUI.

To run the FortiClient diagnostic tool:

1. Go to *Endpoints*.
2. Select a domain or workgroup.
   The list of endpoints is displayed in the content pane.
3. Click one or multiple endpoints, and from the *Action* menu, select *Request Diagnostic Results*.
   The `<number>_Diagnostic_Result` file is uploaded to the following location on your computer: `<drive>:\Program Files (x86)\Fortinet\FortiClientEMS\logs`.

Updating signatures

You can use EMS to request that FortiClient update signatures on the endpoints.

To update signatures:

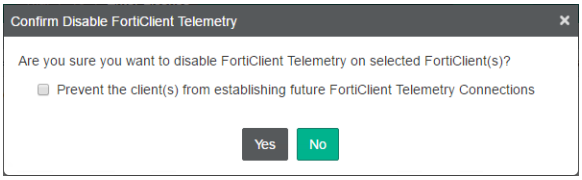
1. Go to *Endpoints*.
2. Select a domain or workgroup.
   The list of endpoints is displayed in the content pane.
3. Click an endpoint, and from the *Action* menu, select *Update Signatures*.
   FortiClient receives the request to update signatures, and downloads the signatures from the Internet.

Deregistering and registering endpoints

You can manually deregister and register endpoints by using EMS.

To deregister endpoints:

1. Go to *Endpoints*.
2. Click a domain or workgroup. A list of endpoints is displayed.
3. Click an endpoint, and from the *Action* menu, select *Deregister*.
   A confirmation dialog box is displayed.



   You can prevent the endpoint from registering in the future by selecting the *Prevent the client(s) from establishing future FortiClient Telemetry Connections* checkbox.
4. Click *Yes* to confirm.
   The endpoint is unregistered with the next FortiClient Telemetry communication.

To register endpoints:

1. Go to *Endpoints*.
2. Click a domain or workgroup. A list of endpoints is displayed.

3. Click an endpoint, and from the *Action* menu, select *Register*.
   The endpoint is registered with the next FortiClient Telemetry communication.

Quarantining endpoints

You can quarantine an endpoint by using EMS. Quarantined endpoints cannot access the network.

To quarantine an endpoint:

1. Go to *Endpoints*.
2. Click a domain or workgroup. A list of endpoints is displayed.
3. Click an endpoint, and from the *Action* menu, select *Quarantine*.
   The endpoint status changes to *Quarantined*, and the endpoint is quarantined with the next FortiClient Telemetry communication.

   You can remove an endpoint from quarantine by right-clicking the endpoint and selecting *Unquarantine*. The endpoint is removed from quarantine with the next FortiClient Telemetry and network access is restored.

Excluding endpoints from management

You can exclude an endpoint from management.

To exclude from management:

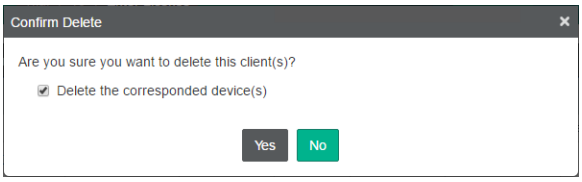
1. Go to *Endpoints*.
2. Click a domain or workgroup. A list of endpoints is displayed.
3. Click an endpoint, and from the *Action* menu, select *Exclude from Management*.
   The endpoint is excluded from management.

Deleting endpoints

You can delete unregistered endpoints from EMS.

To delete endpoints:

1. Go to *Endpoints*.
2. Click a domain or workgroup. A list of endpoints is displayed.
3. If the endpoint has a status of *Registered*, deregister the endpoint.
4. Click an endpoint, and from the *Action* menu, select *Delete Device*.
   A confirmation dialog box is displayed.



5. Click *Yes*.
   The endpoint is deleted from FortiClient EMS.

Endpoint Profiles

You can use the default endpoint profile, or you can create endpoint profiles for many configurations and situations.

Configuring profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups that you create. The default profile is designed to provide effective levels of protection. If you want to use specific features, such as application firewall, you can create a new profile or change the default profile.

Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the role of the endpoint when changing the default profile or creating new profiles.
- Create a separate group and profile for endpoints that require long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the endpoint itself when possible.

Editing the default profile

You can edit the default profile to add or remove settings. You can revert to the default settings at any time by clicking the *Revert to Default* button.

To edit the default profile:

1. Go to *Endpoint Profiles*, and click the *Default* profile. The *Editing Profile: Default* pane is displayed.
2. Configure the settings on the tabs. For a description of the options, see Profile references on page 58.
3. Click *Save Profile* to save the profile.

Creating profiles to configure FortiClient

This section describes how to create a profile that excludes any installation or uninstallation of FortiClient software on endpoints. This type of profile is used to configure FortiClient software on endpoints.

To create profiles:

1. Go to *Endpoint Profiles*, and click the *Add a new profile* button (the + icon). The *Creating New Profile* pane is displayed.
2. In the *Profile Name* box, type a name for the profile.
3. On the *Deployment* tab, leave *FortiClient Deployment* disabled.
4. Configure the settings on the remaining tabs. For a description of the options, see Profile references on page 58.
5. Click *Save Profile* to save the profile.

Creating profiles to deploy FortiClient

You must create a new profile to deploy FortiClient to endpoints. You cannot add a FortiClient installer to the default profile.

You must add FortiClient installers to FortiClient EMS before you can select the installers in a profile. See Adding FortiClient installers on page 85.

The selected FortiClient installer in a profile controls what tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab is always displayed.

You can disable a feature that is included in the installer, and then enable the feature in the profile at a later date. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Feature is installed, but disabled.

To create profiles for FortiClient deployment:

1. Go to *Endpoint Profiles*, and click the *Add a New Profile button* (the + icon). The *Creating New Profile* pane is displayed.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient Deployment options are displayed.
3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Installer*.
	Installer	In the *Installer* list, select a FortiClient installer. If you have not added a FortiClient installer to FortiClient EMS, click *Create a New Installer*. The selected FortiClient installer affects what tabs are displayed for configuration. Only tabs related to features enabled in the FortiClient installer are displayed for configuration.
Schedule		
	Start At	Specify what time to start the installation of FortiClient on endpoints.
	Prompt end user if a reboot is needed during installation	Enable to prompt the end user if a reboot of the endpoint device is needed. Disable to reboot the endpoint device without prompting the user. If no endpoint user is logged into FortiClient, the endpoint is rebooted without a prompt.
Credentials		

	Username	Type the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile you will assign to the AD. The credentials allow EMS to install FortiClient on endpoints by using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Type the password to perform deployment on AD.

4. Set the options on the remaining tabs.
5. Click *Save Profile* to save the profile.

Creating profiles to uninstall FortiClient

You can configure a profile to uninstall FortiClient from endpoints. You must create a new profile for this configuration. You cannot use the default profile to uninstall FortiClient from endpoints.

To create profiles to uninstall FortiClient:

1. Go to *Endpoint Profiles*, and click the *Add a New Profile button* (the + icon). The *Creating New Profile* pane is displayed.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient Deployment options are displayed.
3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Uninstaller*.
Schedule		
	Start At	Specify what time to start uninstalling FortiClient from endpoints.
Credentials		

	Username	Type the username to perform deployment on AD or workgroups. If you are using an AD to uninstall FortiClient on endpoints, you must enter the admin credentials for the AD in the profile. If you are using a workgroup to uninstall FortiClient on endpoints, FortiClient must be registered to FortiClient EMS. Admin credentials are not required. When configuring the profile, know what method (AD or workgoup) is being used to uninstall FortiClient on endpoints. If using an AD, enter the appropriate credentials in the profile you will assign to the AD. The credentials allow EMS to uninstall FortiClient on endpoints by using AD. If the credentials are wrong, the uninstallation fails, and an error displays in EMS.
	Password	Type the password to perform the uninstall on AD or workgroups.

4. Click *Save Profile* to save the profile.

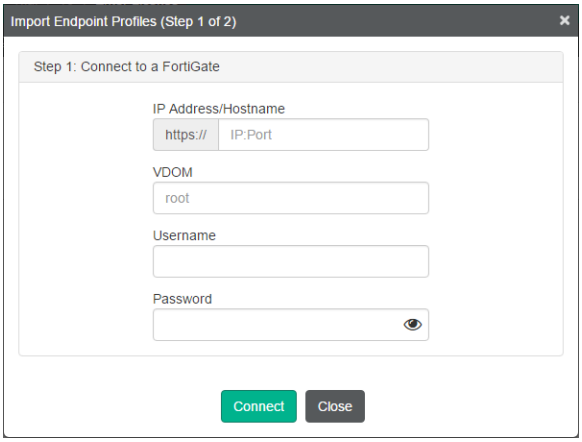
Importing FortiGate profiles

In FortiOS, endpoint profiles are called FortiClient profiles. You can import a FortiClient profile into EMS, and then edit the profile in EMS to add a FortiClient installer or to add configuration information that supports the FortiGate compliance rules.

To import profiles successfully from FortiOS to FortiClient EMS, FortiGate must have the HTTPS port open. In FortiOS, go to *Network* > *Interfaces* > *Restrict Access* > *Enable checkbox for HTTPS*.

To import profiles:

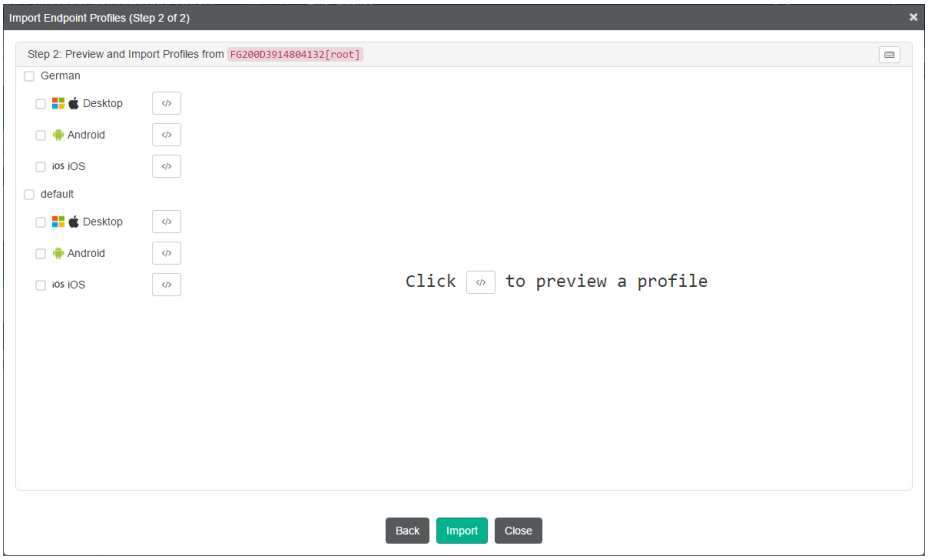
1. Click *Endpoint Profiles* > *Import Profiles from FortiGate*. The *Import Endpoint Profiles* window opens.



2. Complete the following options, and click *Connect*.

IP Address/Hostname	Enter the IP address and port of the FortiGate device from which the profile is being imported, in the format `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the login username for the FortiGate.
Password	Enter the login password for the FortiGate.

The list of FortiClient profiles configured on the FortiGate is displayed.



Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or Mac operating system or devices running an Android operating system. For example, under the default profile, *Desktop*, *Android* and *iOS* profiles are listed. You can click the </> icon beside each profile to preview the settings in XML format.

3. Select the profiles to import into EMS and click *Import*.

   Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the Desktop and iOS profiles, but not the Android profile for a given profile name.

   The selected profiles are imported into EMS and display under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.

4. In the *Endpoint Profiles* page, select an imported profile to edit it.

   The options configured in the profile by the FortiGate administrator are read-only compliance rules. You cannot change them. You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See Adding FortiClient installers on page 85.

5. Edit the options on the tabs.
6. Click *Save Profile*.

Creating profiles with XML

You can configure FortiClient profile settings in FortiClient EMS by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment. For more information about how to configure a profile with XML, see the *FortiClient XML Reference* on docs.fortinet.com.

To create profiles with XML:

1. Go to *Endpoint Profiles*, and click the *Add a New Profile button* (the + icon). The *Creating New Profile* pane is displayed.
2. In the *Profile Name* box, type a name for the profile.
3. Click the *Advanced* button. The *XML* tab is displayed, and the profile configuration displays in XML.
4. Click the *XML Configuration* tab, and click the *Edit* button.
5. Edit the XML.
6. Click *Test XML*.
7. Click *Save Profile* to save the profile.

Creating profiles to automatically upgrade FortiClient

You can create a profile to automatically upgrade FortiClient to the latest patch release. The profile must be configured with an installer that meets the following requirements:

- The FortiClient installer was created in FortiClient EMS 1.2.0 or later.
- The FortiClient installer was created with the latest FortiClient version available for selection in FortiClient EMS at the time the installer was created.
- The FortiClient installer was created with the *Keep software updated to the latest patch release* option enabled.

See Adding FortiClient installers on page 85 for details on creating an installer.

With this configuration, when an upgrade is available, FortiClient downloads it directly from the FortiClient EMS server. Offline FortiClients remain without the upgrade until they contact the FortiClient EMS server.

To create profiles to automatically upgrade FortiClient:

1. Go to *Endpoint Profiles*, and click the *Add a new profile* button (the + icon). The *Creating New Profile* pane is displayed.
2. In the *Profile Name* box, type a name for the profile.
3. On the *Deployment* tab, enable *FortiClient Deployment*.
4. Beside *Assign an*, click *Installer*.
5. From the *Installer* dropdown list, select the desired installer, or use the *Create a New Installer* button.
6. Configure the profile as desired, then click *Save Profile*.

Viewing profiles

When you create endpoint profiles, they are listed under *Endpoint Profiles* in the left pane. You can view the endpoint profiles and their settings.

To view profiles:

1. Go to *Endpoint Profiles*, and click *EMS Profiles*. The list of profiles is displayed in the left pane.
2. Click a profile name. The settings are displayed in the content pane.

Assigning profiles to endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

To assign profiles:

1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign Profile*, and then the profile. A confirmation dialog box is displayed.
3. Click *Yes*. The profile is assigned.

Managing profiles

You can manage profiles from the *Endpoint Profiles* pane.

Editing profiles

When you edit a profile that is assigned to endpoints, the changes are automatically pushed to the endpoints when you save the profile.

To edit profiles:

1. Go to *Endpoint Profiles*, and select a profile. The profile settings are displayed in the content pane.
2. Edit the settings. For a description of the options on the tabs, see Profile references on page 58.
3. Click *Save Profile*. If the profile is assigned to endpoints, the changes are pushed to the endpoints.

Cloning profiles

To clone profiles:

1. Go to *Endpoint Profiles*.
2. Select a profile, and click the *Clone* button. The cloned profile is displayed in the content pane.
3. In the *Profile Name* box, type a name for the profile.
4. Configure the settings on the tabs. For a description of the options, see Profile references on page 58.
5. Click *Save Profile* to save the profile.

Deleting profiles

You cannot delete the default profile.

To delete profiles:

1. Go to *Endpoint Profiles*.
2. Select a profile, and click the *Delete* button. A popup menu is displayed.
3. Click *Delete*. The profile is deleted

Profile references

This section contains descriptions of the tabs and options used to configure profiles.

Profile Name

Option	Description
Profile Name	Type a name for the profile.
Basic	Select to display the basic options for configuration and to configure the profile by using the GUI.
Advanced	Select to display the advanced options for configuration and to configure the profile by using XML on the *XML Configuration* tab.

AntiVirus Protection

Enable antivirus protection. Some options are only displayed if you enable *Advanced* view. Configure the following options:

Options	Description
AntiVirus Protection	Toggle to enable or disable AntiVirus protection.
Real-Time Protection	
Scan Files as They Are Downloaded or Copied to My System	Scan files for threats as they are downloaded or copied to the system.

Options		Description
	On Virus Discovery	• Clean Infected files (Quarantine If Cannot Clean). This option deletes the infected file. • Repair Infected files (Quarantine If Cannot Clean). This option extracts the virus from the infected file. This option will not work with most modern viruses. • Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • Deny Access to Infected Files • Ignore Infected Files
Alert When Viruses Are Detected		If enabled, displays the *Virus Alert* dialog when a virus is detected while attempting to download a file via a web browser. The dialog allows you to view recently detected viruses, and their locations and statuses.
Block Known Communication Channels Used by Attackers		Enable to block known communication channels used by attackers.
Block All Access to Malicious Websites		Block all access to malicious websites. You must select *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab before you can enable this option.
	Use the Exclusion List Defined in the Web Filter Profile	If this checkbox is selected, the exclusion list on the *Web Filter* tab is used. If this checkbox is not selected, you must define exclusions under *Exclusions*.
Scan Compressed Files		Enable to scan compressed files for threats.
	Max Size	Configure the maximum size (in MB) of compressed files to scan. To allow scanning compressed files of any size, enter 0.
	User Process Scanning	Enable user process scanning. Select one of the following: • Scan Files When Processes Read or Write Them • Scan Files When Processes Read Them • Scan Files When Processes Write Them
Scan Network Files		Enable to scan network files for threats.

Options	Description
System Process Scanning	Enable system process scanning. Select one of the following: • Scan Files When System Processes Read or Write Them • Scan Files When System Processes Read Them • Scan Files When System Processes Write Them • Do Not Scan Files When System Processes Read or Write Them
On Demand Scanning	
On Virus Discovery	Select one of the following from the dropdown list: • Clean Infected files (Quarantine If Cannot Clean). This option deletes the infected file. • Repair Infected files (Quarantine If Cannot Clean). This option extracts the virus from the infected file. This option will not work with most modern viruses. • Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • Ignore Infected Files
Integrate FortiClient into Windows Explorer's Context Menu	Adds a *Scan with FortiClient AntiVirus* option to the Windows Explorer right-click menu.
Pause Scanning When Running on Battery Power	Enable to pause scanning when the computer is running on battery power.
Automatically Submit Suspicious Files to FortiGuard for Analysis	Enable to automatically submit suspicious files to FortiGuard for analysis. You do not receive feedback for files submitted for analysis. The FortiGuard team is able to create signatures for any files that are submitted for analysis and determined to be malicious.
Scan Compressed Files	Enable to scan compressed files for threats.
Max Size	Configure the maximum size of compressed files to be scanned in MB. To allow compressed files of any size, enter 0.

Options		Description
	Max Scan Speed on Computers With	Select the minimum amount of memory that must be installed on a computer to maximize scan speed: • 4 GB • 6 GB • 8 GB • 12 GB • 16 GB
Scheduled Scan		Enable scheduled scans.
Scheduled Type		Select *Daily*, *Weekly*, or *Monthly*.
Scan On		If *Weekly* is selected, select the day of the week to perform the scan. If *Monthly* is selected, select the day of the month to perform the scan. Note that if you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.
Start At		Configure the start time for the scheduled scan.
Scan Type		Select *Quick*, *Full*, or *Custom*.
	Quick	Runs the rootkit detection engine to detect and remove rootkits. The quick scan only scans the following items for threats: executable files, DLLs, and drivers that are currently running.
	Full	Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers. If *Full* is selected, you have the following options: • Scan removable media, if present • Scan network drives
	Custom Scan	Runs the rootkit detection engine to detect and remove rootkits. In the *Folder* field, enter the full path of the folder on your local hard disk drive that will be scanned.
Scan Priority		Set to *Low*, *Normal*, or *High*. This refers to the amount of processing power the scan uses and its impact on other processes.
Scan Removable Media		Enable to scan connected removable media, such as USB drives, for threats.
Scan Network Drives		Enable to scan network drives for threats.

Options	Description
Enable Scheduled Scans Even when a Third-Party AV Product Is Present	Enable scheduled scans even when a third party AV product is present.
Exclusions	Enable exclusions from antivirus scanning.
Paths to Excluded Folders	Enter fully qualified excluded folder paths in the provided text box to exclude these folders from antivirus scanning.
Paths to Excluded Files	Enter fully qualified excluded files in the provided text box to exclude these files from antivirus scanning.
File Extensions Excluded from Real-Time Protection	Enter file extensions to exclude from real-time AV protection.
File Extensions Excluded from On Demand Scanning	Enter file extensions to exclude from on demand AV protection.
Other	
Scan for Rootkits	Enable to scan for rootkits. A rootkit is a collection of programs that enable administrator-level access to a computer or computer network. Typically a rootkit is installed on a computer after first obtaining user-level access by exploiting a known vulnerability or cracking a password.
Scan for Adware	Enable to scan for adware. Adware is a form of software that downloads or displays unwanted ads when a user is online.
Scan for Riskware	Enable to scan for riskware. Riskware refers to legitimate programs which, when installed and executed, presents a possible but not definite risk to the computer.
Enable Advanced Heuristics	Enable advanced heuristics. Advanced heuristics is a sequence of heuristics to detect complex malware.
Scan Removable Media on Insertion	Enable to scan removable media (CDs, DVDs, Blu-ray disks, USB keys etc.) on insertion.
Scan Email	Enable to scan emails for threats.

Options	Description
Scan MIME Files (Inbox Files)	Enable to scan MIME files. Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of the email to support the following: • Text in character sets other than ASCII • Non text attachments (audio, video, images, applications) • Message bodies with multiple parts
Enable FortiGuard Analytics	Automatically sends suspicious files to FortiGuard for analysis.
Notify Logged in Users if Their AV Signatures Expired	Enable to notify logged in users if their AntiVirus signatures have expired.

Sandbox Detection

Enable Sandbox Detection. Some options are only displayed if you enable *Advanced* mode. Configure the following options:

Options		Description
Sandbox Detection		Enable or disable Sandbox Detection.
Server		
	IP Address/Hostname	Enter the IP address/hostname of the FortiSandbox unit.
	Wait for FortiSandbox Results before Allowing File Access	Enable to have the endpoint user wait for FortiSandbox scanning results before being allowed access to files. Set the timeout in seconds. Disable to allow the endpoint user to access files before FortiSandbox results are provided.
	Deny Access to File If FortiSandbox Is Unreachable	You have the option to: • Deny Access to Downloaded Files If FortiSandbox Is Offline. • Enter the *Timeout* value in seconds. File Access will be allowed if FortiSandbox results are not received when the timeout expires. Set to `-1` to infinitely restrict access to the file.
Submission		

Options		Description
	All Files Executed from Removable Media	Enable to submit all files executed from removable media.
	All Files Executed from Mapped Network Drives	Enable to submit all files executed from mapped network drives.
	All Web Downloads	Enable to submit all web downloads.
	All Email Downloads	Enable to submit all email downloads.
Remediation		
	Action	Choose either *Quarantine* or *Alert & Notify* infected files.
Exceptions		
	Exclude Files from Trusted Sources	Enable to exclude files from trusted sources.
	Exclude Specified Folders/Files	Enable to exclude specified folders/files.

Web Filter

You must enable *FortiProxy* on the *System Settings* tab to use the *Web Filter* options.

Configuration		Description
Web Filter		Enable or disable web filtering.
General		
	Client Web Filtering When On-Net	Enable Client Web Filtering when onnet.
	Log All URLs	Enable to log all URLs.
	Log User Initiated Traffic	Enable to log user initiated traffic.
Site Categories		

Configuration		Description
	Adult/Mature Content	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard web site for descriptions of the available categories and subcategories.
	Bandwidth Consuming	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard web site for descriptions of the available categories and subcategories.
	General Interest-Business	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard web site for descriptions of the available categories and subcategories.
	General Interest-Personal	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard web site for descriptions of the available categories and subcategories.
	Potentially Liable	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard web site for descriptions of the available categories and subcategories.

Configuration		Description
	Security Risk	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard web site for descriptions of the available categories and subcategories.
	Unrated	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard web site for descriptions of the available categories and subcategories.
	Rate IP Addresses	Enable to rate all IP addresses.
Exclusion List		
Action		Select one of the following actions: • Allow • Block • Monitor
URL		Enter specific URLs to allow, block, or monitor.
Type		Select one of the following types: • Simple • Wildcard • Regular Expression Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.

Application Firewall

Configuration	Description
Application Firewall	Enable or disable application control.
Notification Bubbles on User's Desktop When Applications Are Blocked	Enable notification bubbles when applications are blocked.
Detect & Block Exploits	Enable to detect and block exploits.

Configuration	Description
Categories	Block, allow or monitor the following categories: a. Botnet b. Business c. Cloud.IT d. Collaboration e. Email f. File Sharing g. Game h. General.Interest i. IM j. Industrial k. Mobile l. Network.Service m. P2P n. Proxy o. Remote.Access p. Social.Media q. Special r. Storage.Backup s. Update t. Video/Audio u. VoIP v. Web.Others w. All Other Known Applications x. All Other Unknown Applications
Application Overrides	
Delete	Delete an application.
Add Signature	Add a signature to an application.

VPN

Configuration	Description
VPN	Enable or disable VPN use.
Allow Personal VPN	Enable to allow personal VPN.
Disable Connect/Disconnect	Enable to disable connect/disconnect.

Configuration		Description
Show VPN before Logon		Enable to show VPN before logon.
Use Windows Credentials		Use Windows credentials for VPN.
Minimize Window on Connect		Enable to minimize the window upon connecting.
Show Negotiation Window		Enable to show negotiation window.
Use Vendor ID		Enable to use vendor ID.
	Vendor ID	Enter the vendor ID.
Current Connection		Enable current connection.
Auto-Connect		Enable to automatically connect when you add a VPN tunnel.
	Auto-Connect Only when Off-Net	Enable to only automatically connect when off-net.
Keep Running Max Tries		Enter the maximum number of attempts. It cannot be a negative value.
SSL VPN		Enable SSL VPN.
	DNS Cache Service Control	FortiClient disables Windows OS DNS cache when an SSL VPN tunnel is established. The DNS cache is restored after SSL VPN tunnel is disconnected. If it is observed that FSSO clients do not function correctly when an SSL VPN tunnel is up, use the following XML configuration to control DNS cache.
	Prefer SSL VPN DNS	When disabled, custom DNS server from SSL VPN will not be added to physical interface. When enabled, custom DNS server from SSL VPN will be prepended to physical interface.
IPSec VPN		Enable IPSec VPN.

Configuration		Description
		Enable or disable the following: **a.** Beep if Error **b.** Use Windows Store Certificates **c.** Current User Windows Store Certificates (IPsec only) **d.** Local Computer Windows Store Certificates (IPSec only) **e.** Use Local Certificates **f.** Use Smart Card Certificates **g.** Show Auth Certificates Only **h.** Block IPv6 **i.** Enable UDP Checksum **j.** Disable Default Route **k.** Check for Certificate Private Key **l.** Enhanced Key Usage Mandatory
Add VPN Tunnel		
	Name	Enter a VPN name.
	Type	Select either *SSL VPN* or *IPSec VPN* for the type.
	Remote Gateway	Enter an IP address or hostname.
	Port	Enter the access port.
	Require Certificate	Enable to require a certificate.
Advanced Settings		
	Enable Single User Mode	Enable Single User Mode.
	Enable Invalid Server Certificate Warning	Enable when there is an invalid server certificate.
	Show "Remember Password" Option	Enable to remember your password.
	Show "Always Up" Option	Enable to have the VPN tunnel always up. This is also needs to be enabled on the FortiGate.
	Show "Auto Connect" Option	Enable to automatically connect the VPN tunnel. This is also needs to be enabled on the FortiGate.

Configuration		Description
	On Connect Script	Enable the On Connect Script. Enter your script. This also needs to be enabled on the FortiGate.
	On Disconnect Script	Enable the Disconnect Script. Enter your script. This also needs to be enabled on the FortiGate.

Vulnerability Scan

Configuration		Description
Vulnerability Scan		Enable or disable Vulnerability Scan.
Scan on Registration		Scan endpoints upon registering to a FortiGate.
Scan on Signature Update		Scan endpoints upon updating a signature.
Scan for OS Updates		Scan for OS updates.
Scheduled Scan		Schedule the scan.
	Schedule Type	Configure either *Daily*, *Weekly*, *Monthly*.
	Scan On	Configure the day the scan will run (1st-31st of the month). This only applies if the schedule type is configured to *Monthly*.
	Start At	Configure the time the scan will start.
Automatic Patching		
	Patch Level	When enabled, patches will be installed automatically when vulnerabilities are detected. Select one of the following: • Critical: Patch critical vulnerabilities only • High: Patch high severity, and above, vulnerabilities • Medium: Patch medium severity, and above, vulnerabilities • Low: Patch low severity, and above, vulnerabilities • All: Patch all vulnerabilities. Automatic patching may require endpoint reboot.
Exclusions		

Configuration		Description
	Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check	When enabled, all applications that require the endpoint user to manually patch vulnerabilities are excluded from vulnerability scanning.
	Exclude Selected Applications from Vulnerability Compliance Check	In the *<number> Programs* list, click the applications that you want to exclude, and they are automatically moved to the *<number> Excluded Programs* list. In the *<number> Excluded Programs* list, click the applications that you want to remove from the exclusion list.

System Settings

Configuration	Description
UI	Specify how the FortiClient user interface will appear when installed on endpoints.
Show Dashboard Banner	Enable the dashboard banner.
Password Lock Configuration	Turn on the password lock for FortiClient.
Password	Type a password.
Do Not Allow User to Back up Configuration	Enable to not allow users to back up configuration.
Hide System Tray Icon	Enable to hide the system tray icon.

Configuration	Description
Culture Code	Configure the culture code. Select one of the following: • os-default • zh-tw • cs-cz • de-de • en-us • fr-fr • hu-hu • ru-ru • ja-jp • ko-kr • pt-br • sk-sk • es-es • zh-cn • et-ee • lv-lv • lt-lt • sv-se • da-dk • pl-pl • nb-no
Log	Specify the log settings for FortiClient.
Level	Select one of the following: • Disabled • Emergency • Alert • Critical • Error • Warning • Notice • Information • Debug

Configuration		Description
Features		Enable any (or all) of the following: • AntiVirus • Application Firewall • Telemetry • FSSOMA • Proxy • IPSec VPN • SSL VPN • Update • Vulnerability • Web Filter • Sandbox
Client-Based Logging when On-Net		Turn on client-based logging when onnet. For more information about using the onnet feature, see the *FortiClient Administration Guide*.
Upload Logs to FortiAnalyzer/FortiManager		Turn on to upload FortiClient logs to the FortiAnalyzer or FortiManager device at the specified address or host-name.
	Upload Traffic Logs	Enable to upload traffic logs.
	Upload Vul-nerability Logs	Enable to upload vulnerability logs.
	Upload Event Logs	Enable to upload event logs.
	IP Address/Host-name	Enter the IP address. When connecting to FortiAnalyzer 5.6+, use the format *https://FAZ-IP:port/logging*. Other-wise, use the format *https://FAZ-IP/jsonrpc/fazapi/logs*.
	SSL Enabled	Enable SSL.
	Upload Schedule (minutes)	Configure the upload schedule in minutes.
	Log Generation Timeout (seconds)	Configure the log generation timeout in seconds.
	Log Retention (days)	Configure the number of days to retain logs.
Proxy		
Use Proxy for Updates		Enable to use proxy for updates.

Configuration		Description
	Connect to FDN Directly If Proxy Is Offline	Enable to connect to FDN directly if proxy is offline.
Use Proxy for Virus Submission		Enable to use proxy for virus submission.
	Type	Configure the type. Options include: • http • socks4 • socks5
	IP Address/Hostname	Enter the IP address/hostname.
	Port	Enter the port number.
	Username	Enter the username.
	Password	Enter the password. Enable Show Password to show the password in plain text.
Update		Specify whether to use FortiManager to update FortiClient on endpoints
Use FortiManager for Client Software/Signature Update		Turn on to enable FortiClient EMS to obtain antivirus signatures and software updates from the FortiManager device at the specified IP address or hostname.
	IP Address/Hostname	Enter the IP address/hostname.
	Port	Enter the port number.
	Failover Port	Enter the failover port.
	Timeout	Enter the timeout interval.
	Failover to FDN When FortiManager Is Not Available	Enable failover to FDN when FortiManager is not available.
Auto Patch		Enable auto patch.

Configuration		Description
	Update Action	Select one of the following: • Notify Only The update action will be set to *Disabled*. The Advanced XML configuration should be: `<update_action>disable</update_action>` • Download And Install • Download Only
Scheduled Updates		Enable to configure the update schedule.
	Schedule Type	Select either *Interval* or *Daily* for your schedule time.
	Update Every	Configure the interval.
FortiProxy		Enable FortiProxy (disable only when troubleshooting). You must enable FortiProxy to use the Web Filter options as well as some AntiVirus options.
HTTPS Proxy		Enable HTTPS Proxy.
	HTTP Timeout	Enter the HTTP timeout interval.
POP3 Client Comforting		Enable POP3 Client Comforting.
POP3 Server Comforting		Enable POP3 Server Comforting.
SMTP Client Comforting		Enable SMTP.
Self Test		Enable SelfTest. You have the option to *Notify* the *Last Port*.
	Notify	Enable Notify and enter the last port.
	Last Port	Last port number.
Endpoint Control		Specify settings for the endpoints.
Show Bubble Notifications		Enable to show bubble notifications.
Show Profile Details		Enable to show profile details.
Silent Registration		Turn on to enable silent registration of endpoints, which means that endpoints are registered without user interaction. Turn off to require user interaction to register endpoints.

Configuration		Description
Log off When User Logs Out of Windows		Turn on to log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.
Disable Unregister		Turn on to forbid users from unregistering FortiClient from FortiClient EMS. Turn off to allow users to unregister FortiClient from FortiClient EMS.
	Disable FortiGate Switch	Enable to disable the FortiGate switch.
Onnet Subnets		Turn on to enable onnet subnets.
	List of IP Addresses/Masks	Enter IP addresses/mask to connect to onnet subnets.
Gateway MAC Address		Enable gateway MAC address.
	Gateway Mac Addresses	Enter MAC addresses.
Other Options		
Install CA Certificate on Client		Turn on to select and install a CA certificate on the FortiClient endpoint. You can add certificates by going to *View* > *CA Certificate Management*.
FortiClient Single sign-On mobility agent		Turn on to enable the single sign-on mobility agent.
	IP Address/Host-name	Enter the IP address or hostname.
	Port	Enter the port number.
	Pre-shared Key	Enter the pre-shared key.
WAN Optimization		Enable WAN optimization.
	Maximum Disk Cache Size	Select either *512* or *1024* MB.
iOS		
Distribute Configuration Profile (.mobileconfig file)		Enable and browse for your `.mobileconfig` file to distribute the configuration profile.
Privacy		

Configuration		Description
	Send Usage Statistics to Fortinet	Sending usage statistics to Fortinet will be used to improve our product quality and user experience.

XML Configuration

Configuration	Description
XML Editor	Configure using the XML editor. For more information, see the FortiClient XML Reference Guide available in the Fortinet Document Library.

Gateway IP Lists

Gateway IP lists are useful when you are using FortiClient EMS integrated with FortiGate. If you are using FortiClient EMS without FortiGate, you are not required to use gateway IP lists.

You can use gateway IP lists to specify what IP addresses or fully qualified domain names (FQDN) and ports that FortiClient endpoints can use to connect FortiClient Telemetry to FortiGate, EMS, or both FortiGate and EMS. You can create one or more gateway IP lists and assign them to domains or workgroups.

After deploying FortiClient to endpoints, FortiClient uses the gateway IP list to try and connect or register FortiClient Telemetry to FortiGate or EMS. This registration is based on the gateway IP list received from EMS.

Even if the endpoint is already registered to a FortiGate, you can still assign a gateway IP list to endpoints. You can also update existing gateway IP lists as required. The updates will be pushed to FortiClient endpoints with the next Telemetry communication.

Creating gateway IP lists

Gateway IP lists are useful when you are using FortiClient EMS integrated with FortiGate. If you are using FortiClient EMS without FortiGate, you are not required to use gateway IP lists.

You can create one or more gateway IP lists. Each list can contain IP addresses for multiple FortiGate units.

To create gateway IP lists:

1. Go to *Gateway IP Lists*.
2. Click the *Add a new IP list* button (the + icon).
3. Configure the following:

Name	Enter a name for the list.
Export XML	Available after you save the list. Click to export the list to a configuration file in XML format.
Comment	Enter additional comments (optional).
IP List	Enter the IP address and port for FortiGate devices by using the following format: IP:port. You can also use a Fully Qualified Domain Name (FQDN). Click + to add additional IP addresses, and use the arrow keys to order the IP addresses in the list.
Use Connection Key	Enable the registration key for FortiGate devices that FortiClient endpoints can use for registration.

	Connection Key (Optional)	Enter the registration key.
	Confirm Connection Key	Re-enter the registration key to confirm.
Monitored by EMS		Select an option from the dropdown list. Users can configure this IP address in the *View* > *Settings* page.

4. Click *Save*.
   After you save the list, the *Export XML* button is displayed.

Exporting gateway IP lists to XML

After you create and save a gateway IP list, the *Export XML* button is displayed, and you can export the list to a configuration file in XML format.

To export gateway IP lists to XML:

1. Go to *Gateway IP Lists*.
2. Click a list to open it.
3. Click the *Export XML* button.
   A `<filename>.conf` file is downloaded to your computer. Following is an example of the XML:

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
   <endpoint_control>
      <fortigates>
         <fortigate>
            <name>FortiGate</name>
            <registration_password></registration_password>
            <addresses>1.1.1.1:8013</addresses>
         </fortigate>
      </fortigates>
      <notification_server>
         <registration_password></registration_password>
         <address>1.1.1.1:8013</address>
      </notification_server>
   </endpoint_control>
</forticlient_configuration>
```

Viewing gateway IP lists

When you create gateway IP lists, they are listed under *Gateway IP Lists* in the left pane. You can view the gateway IP lists and their settings.

To view gateway IP lists:

1. Go to *Gateway IP Lists*. The gateway IP lists are displayed in the left pane.
2. Click the name of a gateway IP list. The settings are displayed in the content pane.

Assigning gateway IP lists to endpoints

After creating a gateway IP list, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data registration process has started, the endpoint will register to a FortiGate or EMS, based on the gateway IP list.

To assign gateway IP lists to endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Assign FortiClient Telemetry Gateway IP List* > *Select List*.

Viewing assigned gateway IP lists

To view assigned gateway IP lists:

1. Select an endpoint.
2. View the *Summary* > *Configuration* > *IP List* area.

Deployment

You can use FortiClient EMS to deploy FortiClient on the endpoint devices that are part of an Active Directory (AD) server. Deploying FortiClient from FortiClient EMS requires the following steps:

- Preparing the AD server for deployment
- Deploying FortiClient on endpoint devices

After FortiClient is deployed on endpoints, and endpoints are connected to FortiClient EMS, you can update endpoints by editing the profiles associated with endpoints.

You can also use FortiClient EMS to uninstall and upgrade FortiClient on endpoint devices that are part of an AD server.

You cannot use workgroups to deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints, endpoints are connected to FortiClient EMS, and FortiClient is registered to FortiClient EMS, you can use work-groups to uninstall and update FortiClient on endpoints.

Preparing the AD server for deployment

Before you can successfully deploy a FortiClient installation, ensure that you install and prepare the AD server as follows:

- Configure a group policy on the AD server
- Configure the required Windows services on the AD server
- Create deployment rules for Windows firewall
- Configure Windows firewall domain profile settings

Configuring a group policy on the AD server

To configure a group policy on the AD server:

1. On the AD server, open *Group Policy Management*.
2. Right-click the *Default Domain Policy* setting. The Group Policy Management Editor opens.
   A new policy will be applied to the entire AD domain. Alternatively, you can create a new Group Policy Object, and link it to one or more organizational units (OU) in the AD server that contains the endpoint computes on which FortiClient will be deployed.

Configuring required Windows services

To configure required Windows services:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *System Services*.

2. In the right panel, select the following:
    a. Task Scheduler: Automatic
    b. Windows Installer: Manual
    c. Remote Registry: Automatic

Creating deployment rules for Windows firewall

To create deployment rules for Windows firewall:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Windows Firewall with Advanced Security* > *Inbound Rules*.
2. Right-click *Inbound Rules* and select *New Rule*.
3. Select *Predefined* from the dropdown list and select *File and Printer Sharing*.
4. Click *Next*.
5. Ensure that the *File and Printer Sharing (SMB-In)* box is selected and click *Next*.
6. Select *Allow the connection* and click *Finish*.
7. Repeat steps 1 to 2.
8. Select *Predefined* from the dropdown list and select *Remote Scheduled Tasks Management* and click *Next*.
9. Ensure that the *Remote Scheduled Tasks Management (RPC)* checkbox is selected and click *Next*.
10. Select *Allow the connection* and click *Finish*.

Configuring Windows firewall domain profile settings

To configure Windows firewall domain profile settings:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Administrative Templates* > *Network* > *Network Connections* > *Windows Firewall* > *Domain Profile*.
2. Select *Allow inbound file and printer sharing* exception:
    a. Right-click and select *Edit*.
    b. Enable the radio button.
    c. Provide the IP address of the EMS server in the text box.
    d. Allow unsolicited incoming messages from these IP addresses.
    e. Click OK.
3. Select *Allow inbound file and remote administration* exception.
   Repeat steps listed in step 2 above to create an exception.
4. Select *Allow ICMP Exceptions*:
    a. Right-click and select *Edit*.
    b. Enable the radio button.
    c. Select the *Allow inbound echo request* checkbox.
    d. Click *OK*.

To deploy the group policy manually, execute `gpupdate /force` on the AD server to update the group profile on all endpoint clients.

Execute `gpresult.exe /H gpresult.html` on any AD client to view the group policy deployed on the endpoints.

Preparing Windows endpoints for FortiClient deployment

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic

The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
- Remote Scheduled Tasks Management (RPC)

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in Software Manager. Go to *View* > *Software Manager*.

Deploying FortiClient on endpoint devices

Before you can successfully deploy a FortiClient installation from FortiClient EMS by using an AD server, you must have prepared the AD server. See Preparing the AD server for deployment on page 81.

To deploy FortiClient by using AD servers

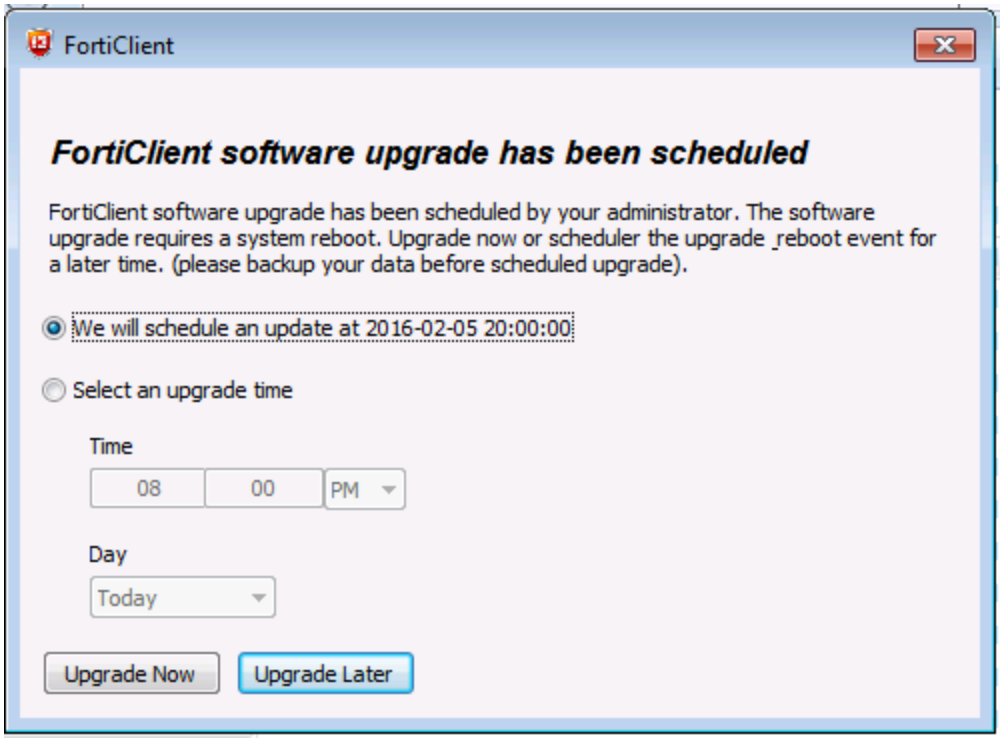
1. Add the AD server to FortiClient EMS by adding a domain. See Adding endpoints using an Active Directory domain service on page 37.
2. Add a FortiClient installer package to FortiClient EMS. See Adding FortiClient installers on page 85.
3. Add a profile, select the FortiClient installer package, and configure FortiClient features in the profile. See Creating profiles to deploy FortiClient on page 52.
4. Assign the profile to a branch of the AD domain to push the FortiClient installation process on the endpoint devices. See Assigning profiles to endpoints on page 57.
5. Verify the deployment by monitoring FortiClient registrations to the FortiClient EMS.

Deploying FortiClient upgrades from EMS

You can deploy a FortiClient software update from EMS. A prompt will appear in the FortiClient endpoint when an installer package is requested to be deployed. The prompt will request the user to do either of the following:

a. Upgrade Now
If this option is selected, it will perform the upgrade and will automatically restart your computer.

b. Upgrade Later
If this option is selected, you can indicate the time to start the upgrade. Otherwise, the default time is at 8:00PM. Your computer will automatically restart after the upgrade has finished.



c. No Option
If no option is selected, the upgrade will occur, by default at 8:00PM.

After FortiClient EMS uninstalls the previous version, it will ask if the user would like to reboot. The prompt will request the user to do either of the following:

a. Reboot Now
If this option is selected, the reboot will occur immediately.

b. Reboot Later
If this option is selected, you can indicate the time to start the reboot.

c. Cancel Reboot
If this option is selected, you can cancel the reboot request and reboot at your discretion.

Software Manager

FortiGuard Distribution Network

FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN) to provide access to FortiClient installers you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS. See Downloading FortiClient installers on page 85.

Downloading FortiClient installers

You can download FortiClient installers from the following locations to use with FortiClient EMS:

- Fortinet Customer Service & Support: https://support.fortinet.com
  Requires a support account with a valid support contract. Download the Microsoft Windows (32-bit/64-bit) or the Mac OS X installation file.
- FortiClient homepage: www.forticlient.com
  Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.

Adding FortiClient installers

When you add a FortiClient installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

When you add a FortiClient installer to FortiClient EMS, an installer for the Windows operating system and an installer for the OS X operating system are added to FortiClient EMS.

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

To add FortiClient installers:

1. Go to *View* > *Software Manager*. The *FortiClient Software Manager* pane is displayed.
2. Click the + *Add* button.
3. On the *General* tab, set the following options:

Name	Type the FortiClient installer name.
Notes	(Optional) Type any notes about the FortiClient installer.

FortiClient Version	Select the FortiClient version to install. Click *Upload* to add a custom FortiClient installer.
Patch Version	Select the specific FortiClient patch version to install.
Keep software updated to the latest patch release	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This field is only available for the latest FortiClient version FortiClient EMS can access from FortiGuard. This option is not available if an older FortiClient version is selected.

4. On the *Components* tab, set the following options:

Security Fabric Agent (Mandatory Feature)	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scanning enabled.
Secure Access Architecture	Enable to install FortiClient with SSL VPN and IPsec VPN enabled. Disable to omit SSL VPN and IPsec VPN support from the FortiClient installer.
Additional Security Features	Enable to select one, two, or all of the following features: • AntiVirus • WebFiltering • Application Firewall • Single Sign-On mobility agent Disable to exclude the features from the FortiClient installer.

5. On the *Telemetry* tab, set the following options:

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway IP list you want to use. The gateway IP list defines the IP address for FortiGate and includes the IP address for EMS as well. You must define a FortiClient Telemetry gateway IP list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box is displayed, and you can click *OK* to create a list.

6. On the *Advanced* tab, set the following options:

Automatic registration	Enable to configure FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS or FortiGate.
Desktop shortcut	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint device.
Start menu shortcut	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint device.

7. Click *Save*. The FortiClient installer is added to FortiClient EMS and displayed on the *FortiClient Software Manager* pane.

Uploading custom FortiClient installers

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you might need to manually download a FortiClient installer and add it to FortiClient EMS. For more information, see FortiGuard Distribution Network on page 85.

To add custom FortiClient installers to FortiClient EMS:

1. Download a FortiClient installer. See Downloading FortiClient installers on page 85.
2. Go to *View* > *Software Manager*. The *FortiClient Software Manager* pane is displayed.
3. Click *Add*. The *Add Installer* dialog box is displayed.
4. On the *General* tab, set the following options:

Name	Type the FortiClient installer name.
Notes	(Optional) Type any notes about the FortiClient installer.

5. In the *FortiClient Version* list, select *Upload*.
   Options related to uploading are displayed.
6. Set the following options:

Windows Installers	Enable to upload FortiClient installers for the Windows operating system.
64 bit Installer	Click the *Browse* button to locate and select a custom 64-bit installer for the Windows operating system.
32 bit Installer	Click the *Browse* button to locate and select a custom 32-bit installer for the Windows operating system.
Mac OS X Installers	Enable to upload a FortiClient installer for the OS X operating system.
FortiClient Installer	Click the *Browse* button to locate and select a custom installer for the OS X operating system.

7. On the *Telemetry* tab, set the following options:

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway IP list to use. The gateway IP list defines the IP address for FortiGate and includes the IP address for EMS as well. You must define a FortiClient Telemetry gateway IP list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box is displayed, and you can click *OK* to create a list.

8. Click *Save*. The installer is added to FortiClient EMS and displayed on the *FortiClient Software Manager* pane.

Viewing installers in FortiClient Software Manager

After you add FortiClient installers to FortiClient EMS, you can view them in the FortiClient Software Manager.

To view FortiClient installers:

1. Go to *View* > *Software Manager*.
   The *FortiClient Software Manager* pane displays the available installers.

Available Installers	Lists the following information about each installer: • Operating system (Windows or OS X) • Version of FortiClient software • Name of the FortiClient installer • Location of the FortiClient installer FortiClient EMS. Endpoint users can access this location to download and install FortiClient on endpoints.
Add	Click to add a FortiClient installer.
Refresh	Click to refresh the list of FortiClient installers.
X	Click to delete the FortiClient installer.

Deleting FortiClient installers

To delete FortiClient installers:

1. Go to *View* > *Software Manager*. The *FortiClient Software Manager* pane is displayed.
2. Click the *Delete* (the x icon) button on the right side of the installer name.
   A confirmation dialog box is displayed.
3. Click *Yes*.
   The FortiClient installer is deleted from FortiClient EMS.

User Management

This section describes the default user accounts and permissions for FortiClient EMS. It also describes how to change the administrator password and how to configure Windows users.

Default user account and permissions

The default user named *admin* has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment.

The *admin* user has access to all configured Windows and LDAP servers and users and has the authority to configure user privileges and permissions. If you are not authorized for certain tasks or devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

Viewing users

You can view the default user named *admin* as well as all of the users that you have added to FortiClient EMS.

To view users:

1. Go to *View* > *User Management*.
2. Click the *Administration* tab.
   The following information is displayed:

+Add	Add a new user.
Name	Name of the user.
Access	Type of user access.
Type	Type of user.

Configuring User Management

Changing the admin password

By default, the password is blank for the user account named *admin*. You should add a password to increase security.

To change the admin password:

1. Go to *View* > *User Management*.
2. Select the *Admin* account.
3. Click *Change Password* from the toolbar. Change your password.
4. Click *Save*.

Configuring Windows user accounts

You can configure Windows users to have no access to FortiClient EMS, or you can configure Windows users to have administrator access to FortiClient EMS.

The list of Windows users is derived from the server on which FortiClient EMS is installed. If you want to add more Windows users, you must add them to the server.

To configure Windows users:

1. Go to *View* > *User Management*.
2. Click the *+Add* button from the toolbar.
3. Expand the *Add User* dropdown list.
4. Select the Windows user.
5. Perform one of the following actions:
    a. Select the specific domain access for the user. For a description of the permissions, see Default user account and permissions on page 89.
    b. Configure the permissions. For a description of the options, see User Management reference on page 92.
6. Click *Save*.

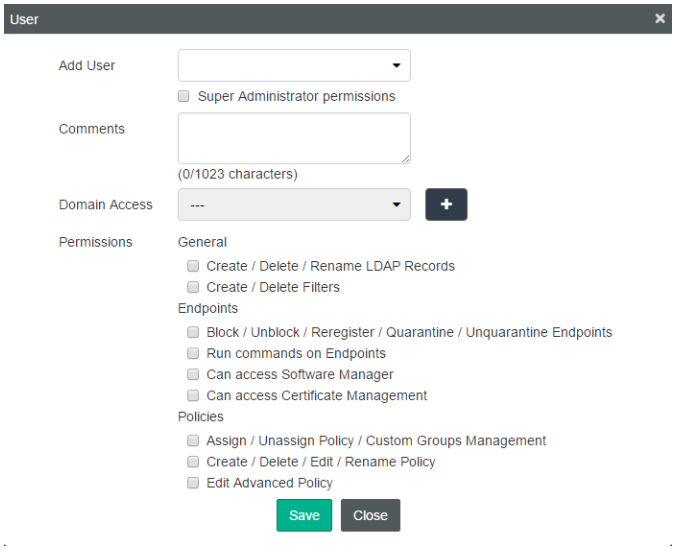
Configuring LDAP user accounts

The list of LDAP users is derived from the server on which FortiClient EMS is installed. If you want to add more LDAP users, you must add them to the server.

To configure LDAP users:

1. Go to *View* > *User Management*.
2. Click the *+Add* from the toolbar.
3. Expand the *Add User* dropdown list.
4. Select the LDAP user.
5. Perform one of the following actions.
6. Configure the options.
    a. Select the specific domain access for the user. For a description of the permissions, see Default user account and permissions on page 89.
    b. Configure the permissions. For a description of the options, see User Management reference on page 92.

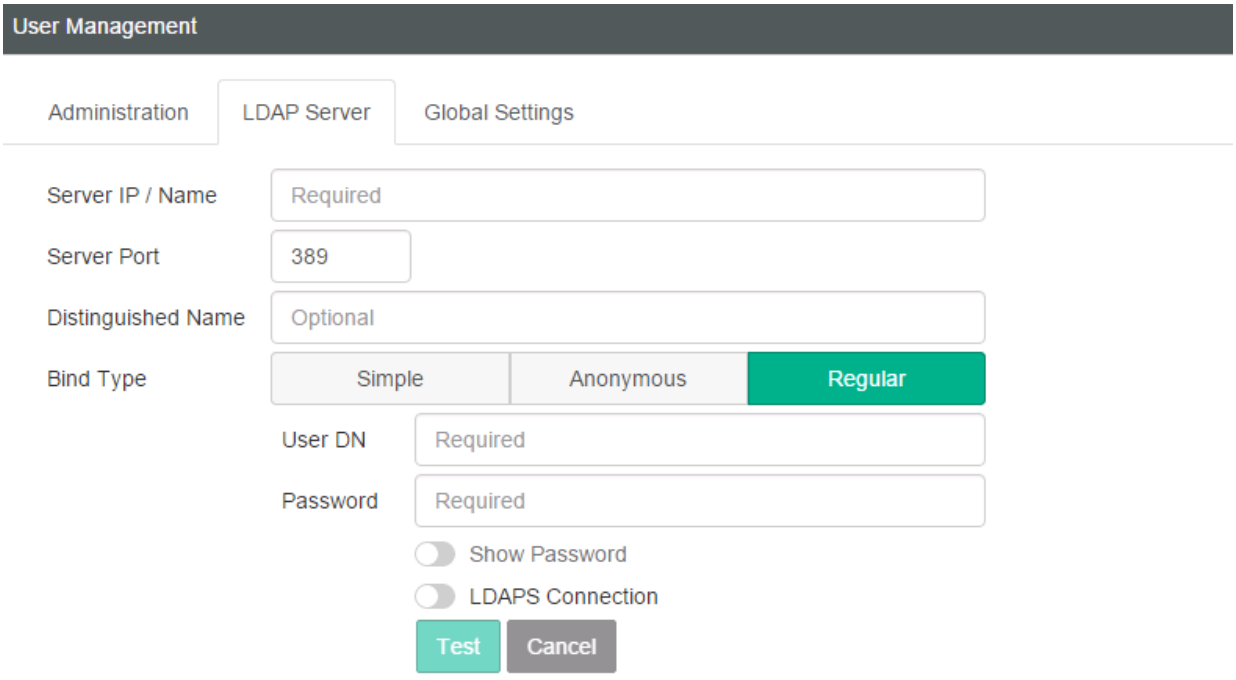
7. Click *Ok*.



Configuring LDAP server

To add an LDAP server:

1. Go *View* > *User Management*, and click the *LDAP Server* tab. The settings are displayed.



2. Configure the following options:

Server IP/Name	Enter the server IP address or name.

Server Port		Enter the server port.
Distinguished Name		Enter a distinguished name.
Bind Type		Select *Simple*, *Anonymous* or *Regular* for the bind type.
	Username	Appears when the *Regular* bind type is selected. Enter the username.
	Password	Appears when the *Regular* bind type is selected. Enter the password.
	Show Password	Enable to show the password.
	LDAPS Connection	Enable the LDAPS connection.

3. Click *Test* to check the LDAP server settings.
4. Click *Save*.

Configuring Global Settings

To configure Global Settings:

1. Go to *View* > *User Management*.
2. Click *Global Settings*.
3. Set the following option:

Inactivity Timeout	Specify how long to keep inactive users logged into FortiClient EMS. When the time expires, the user is automatically logged out of FortiClient EMS. Type 0 to keep inactive users logged into FortiClient EMS indefinitely.

4. Click *Save*.

User Management reference

This section contains descriptions of the fields used to configure user management.

Windows/LDAP users

Following is a description of the fields on the *View* > *User Management* > *Add* > *Windows/LDAP User*.

Option	Description
Add Windows/LDAP User	Select the Windows/LDAP user for whom you want to configure permissions for FortiClient EMS.

Option		Description
Super Administrator permissions		Enable the Super Administrator feature to give the new Windows/LDAP user Super Administrator permissions.
Comments		Enter optional comments/information for the Windows/LDAP user.
Domain Access		Select or add domain access for the Windows or LDAP user and configure their permissions. If you choose one or more domains in the domain access field, you will need to select specific permissions.
Permissions		Use the settings to configure permissions to FortiClient EMS for the selected Windows/LDAP user.
General		
	Create / Delete / Rename LDAP Records	Select to allow the Windows user to create, delete, and rename LDAP records. Clear to disable this permission.
	Create / Delete Filters	Select to allow the Windows user to create and delete filters. Clear to disable this permission.
Endpoints		Use the following options to configure permissions for the selected Windows user.
	Block / Unblock / Deregister / Quarantine / Unquarantine Endpoints	Select to allow the Windows user to block, unblock, deregister, quarantine, and unquarantine endpoints. Clear to disable this permission.
	Run commands on Endpoints	Select to allow the Windows user to run commands on endpoints. Clear to disable this permission.
	Can access Software Manager	Select to allow the Windows user to access the *View* > *Software Management* options. Clear to disable this permission.
	Can access Certificate Management	Select to allow the Windows user to access the *View* > *CA certificate Management* options. Clear to disable this permission.
Policies		

Option		Description
	Assign / Unassign Policy / Custom Groups Management	Select to allow the Windows user to assign to endpoints and unassign profiles from endpoints as well as manage custom groups. Clear to disable this permission.
	Create / Delete / Edit / Rename Policy	Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission.
	Edit Advanced Policy	Select to allow the Windows user to use the advanced settings when editing a profile. Clear to disable this permission.

View Menu

This section describes the options in the *View* menu.

License upgrades or renewals

Contact Fortinet Support to upgrade or renew your FortiClient EMS license. After you have the license file, you can add it to FortiClient EMS.

To upgrade or renew the FortiClient EMS license:

1. Go to *View* > *Upgrade License*. The *Add FortiClient EMS License* pane is displayed.
2. Click *Browse*, and locate the license key file.
3. Click *Upload File*.

CA certificate management

You can import CA certificates into FortiClient EMS.

Importing certificates

To import certificates:

1. Go to *View* > *CA Certificate Management*.
2. Select *Import*.
3. In the *Certificate Upload* window, select either:
   a. *Manual Upload*: If you select this option, click *Browse* to locate the certificate.
   b. *Import from FortiGate*: If you select this option, you will be required to enter the following information:

Server IP/Hostname	Enter the server IP/Hostname in the following format: `<ip address> : <port>`.
VDOM	Enter the VDOM.
Username	Enter the username.
Password	Enter the password.

4. Click *Import* to import the certificate.

Database management

You can back up and restore the FortiClient EMS database.

Backing up the database

To back up the database:

1. Go to *View* > *Database Management*. The *Database Backup/Restore* pane is displayed.
2. On the *Backup* tab, set the following options:

Password	Type a password for backing up and restoring the database.
Confirm Password	Retype the password to confirm the password.

3. Click *Backup Database*.
   The database is backed up.

Restoring the database

To restore the database:

1. Go to *View* > *Database Management*. The *Database Backup/Restore* pane is displayed.
2. On the *Restore* tab, click *Browse*.
3. Locate the database backup file, and click *Open*.
4. In the *Password* box, type the password used to back up the database.
5. Click *Restore Database*.
   When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
6. Wait for the restored database to be reloaded.

Logs

You can view the log messages generated by FortiClient EMS and download raw logs.

Viewing logs

To view log messages:

1. Go to *View* > *View Logs*. The *Logs* pane is displayed.
2. Click the *Filter* icon in each column heading to apply filters.

3. Click *Clear Filters* to remove the filters.

Downloading raw logs

You can download the raw logs generated by FortiClient EMS.

To download raw logs:

1. Go to *View* > *View Logs*. The *Logs* pane is displayed.
2. Click *Raw Logs*.
3. Click the calendar icon in the *Start Date* and *End Date* boxes to select a start date and end date for the logs that you want to download.
4. In the *Levels* dropdown list, select one or more levels of logs to include.
5. In the *Sources* dropdown list, select one or more sources to include.
6. In the *Message* box, type the log message or messages to include. Leave blank to include all log messages.
   If you want to exclude the log message, enable the *NOT* option.
7. Click the *Calculate Size* button to view the size of the download.
8. Click *Download*.
   A zip of the raw logs is downloaded to your computer.

Settings

This section describes FortiClient EMS settings.

Configuring Server Settings

FortiClient EMS installs with a default IP address and port configured. You can change the IP address and port, and configure other server settings for FortiClient EMS.

To configure Server Settings:

1. Go to *View* > *Settings*.
2. Select *Server Settings*, and configure the following options:

Host Name	Displays the host name for the FortiClient EMS server.
Listen on IP Addresses	Displays the IP addresses for the FortiClient EMS server. FortiClient will register to the FortiClient EMS on the specified IP address.
Listen on Port	Displays the default port for the FortiClient EMS server. You can change the port by typing a new port number. FortiClient will register by using the specified port number.
EMS has a FQDN	Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS server.

EMS FQDN	Displayed when *EMS has a FQDN* is turned on. Type the FQDN for the FortiClient EMS server. FortiClient can register by using either the specified IP address in the *Listen on IP Addresses* option or the specified FQDN.
FortiClient Telemetry Connection Key	Add the FortiClient Telemetry connection key for FortiClient EMS. FortiClient must provide this key during registration.
Confirm Key	Add the registration key for FortiClient EMS again to confirm the key.
Keep Alive Interval	Each registered FortiClient sends a short keep-alive message to FortiClient EMS at the specified interval.
Full Keep Alive Interval	Each registered FortiClient sends a full keep-alive message to FortiClient EMS at the specified interval.
License Timeout	A license seat is consumed by each registered FortiClient. If a FortiClient endpoint unregisters from EMS, the license seat is retained in anticipation that the FortiClient endpoint will re-register. If the FortiClient endpoint does not re-register, within the given timeout, its registration record will be removed from EMS. If the FortiClient endpoint is removed, switched off, becomes offline etc. and does not reconnect to EMS within a given timeout, the FortiClient endpoint will be removed from EMS even if it is still registered to EMS.

DHCP Onnet/Offnet	Enable to monitor endpoints within the company network (onnet). Endpoints registered to FortiClient EMS from outside the company network (offnet). There are two settings in EMS that would affect the FortiClient onnet/offnet status: **1.** DHCP onnet/offnet setting in EMS **2.** Subnet setting in EMS Onnet/Offnet Matrix:

DHCP Onnet/Offnet Setting	Subnet Setting	DHCP 224 Option	Result
off	no	N/A	onnet
off or on	yes, match	N/A	onnet
off	yes, not match	N/A	offnet
on	yes or no	option configured	onnet

Notes:
Subnet values:

```
no: subnet setting in EMS is disabled
yes: subnet setting in EMS is configured
match: client has an IP in the configured EMS subnet
not match: client has IP not in the configured EMS
    subnet
```

Examples on how EMS determines the status for the endpoint:

- The endpoint has a status of offline when the endpoint cannot connect FortiClient Telemetry to EMS, and the endpoint is outside one of the onnet networks.
- The endpoint has a status of offline but onnet when the endpoint cannot connect FortiClient Telemetry to EMS. However, the endpoint is inside one of the onnet networks.

Option 224 can have any serial number of a Fortinet device. EMS assumes FortiClient is behind a FortiGate, and it is onnet with that FortiGate.

Remote Administration/HTTPS Access	Specify settings for remote administration access to FortiClient EMS. Turn remote HTTPS access to FortiClient EMS console on and off. When enabled, type a host name in the *Custom Host Name* box to let administrators use a browser and HTTPS to log into the FortiClient EMS console. When disabled, administrators can only log into FortiClient EMS console on the server.
Pre-defined Host Name	Displays the pre-defined host name. The name cannot be changed.

Custom Host Name	Available when *HTTPS Access* is turned on. Displays the pre-defined host name of the server on which FortiClient EMS is installed. You can customize the host name. When you change the host name, the web server restarts.
FortiClient Download URL	FortiClient installers created on FortiClient EMS will be made available for download at the URL.
Open port 10443 in Windows Firewall	Turn on to open port 10443, and turn off to close port 10443. Port 10443 is used to download FortiClient.
SSL Certificate	Displays the SSL certificate currently imported. If you have not imported a SSL certificate, a *No SSL certificate imported* message is displayed.
New SSL Certificate File	Upload a new SSL certificate.
New SSL Private Key	Upload a new SSL private key.
User Inactivity Timeout	Configure the user inactivity timeout in hours.

3. Click *Save*.

Configuring Log Settings

You can specify what level of log messages to capture in the logs for FortiClient EMS. You can also specify when to automatically delete logs and alerts.

To configure Log Settings:

1. Go to *View* > *Settings*.
2. Under *Log Settings*, configure the following options:

Log Level	Select the level of messages to include in FortiClient EMS logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS logs.
Auto Remove Logs	Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted.
Remove All Logs	Click to immediately delete all FortiClient EMS logs.
Auto Remove Alerts	Type the number of days that you want to keep alerts. For example, if you type 30, alerts will be kept for 30 days. Any alerts older than 30 days are automatically deleted.
Remove All Alerts	Click to immediately delete all FortiClient EMS alerts.

3. Click *Save*.

Configuring FortiGuard settings

To configure FortiGuard settings:

1. Go to *View* > *Settings*.
2. Click *FortiGuard*, and configure the following options:

Use FortiManager for Client Software/Signature Update		Turn on to use FortiManager for updating FortiClient software or signatures. You must specify the IP address or host name for FortiManager as well as the port number.
	IP Address/Host Name	Enter the IP address/host name.
	Port	Configure the port number.
	Failover Port	Configure the failover port.
	Timeout	Configure the timeout interval (in seconds).
	Failover to FDN when FortiManager is not available	Enable failover to FDN when FortiManager is not available.
Use Proxy for Updates		Turn on to specify a proxy for updates to FortiClient software.
	IP Address/Host name	Enter the IP address/host name.
	Port	Configure the port.
	Username	Configure the username. This is optional.
	Password	Configure the password.

3. Click *Save*.

Configuring endpoint settings

To configure endpoint settings:

1. Go to *View* > *Settings*, and click *Endpoint Settings*.
2. Enable *Automatically upload user avatars to FortiClient EMS*.
   When enabled, FortiClient uploads user avatars to all FortiGate units, FortiAnalyzer units, and EMS servers it is registered to.
3. Click *Save*.

Configuring the pre-login banner

When you enable the pre-login banner, a message will appear prior to a user logging into EMS.

To enable and configure a pre-login banner:

1. Go to *View* > *Settings*.
2. Under *Pre-Login Banner*, enable *Enable Pre-login Banner*.
3. In the *Banner Message* box, type your message.
4. Click *Save*.

Configuring mail alert settings

You can set up an SMTP server to enable alerts for EMS or endpoint events. When an alert is triggered, an email notification will be sent.

To configure email alerts and an SMTP server:

1. Go to *View* > *Settings* > *E-mail Alerts*.
2. Enable *Send E-mail Alerts for the Following EMS Events* or *Send e-mail alerts for the following endpoint events*, and set the following options:

Notify when new EMS versions are available for deployment	New EMS versions are available.
Remind me everyday for 2 weeks	Enable to remind you when new EMS versions are available everyday for two weeks.
Notify when new FortiClient versions are available for deployment	New FortiClient versions available for deployment.
Remind me everyday for 2 weeks	Enable to remind you when new FortiClient versions are available everyday for two weeks.
Notify when EMS license is expiring or expired	Expiring or expired EMS license.
Notify when EMS fails to sync with LDAP domain(s)	EMS does not sync with LDAP domains.
Notify when less than 10% of client licenses left	Enable to be notified when there are less than 10% of client licenses left.
Notify when out of client licenses	Enable to be notified when you run out of client licenses.

3. Enable *Send e-mail alerts for the following endpoint events* and set the following options:

Send email alerts every	Configure the time interval email alerts are sent. Options include: • 1 min • 5 mins • 10 mins • 15 mins • 30 mins • 1 hour • 2 hours • 6 hours • 12 hours • 1 day
Malware is detected	Malware detected.
Repeated malware is detected	Same malware is detected on the same machine in the last 24 hours.
Multiple malwares detected	Different malware is detected on the same machine in the last 24 hours.
Malware outbreak detected	Same malware is detected on different endpoints in the last 24 hours.
Zero-day malware detected by FortiSandbox	Previously unknown computer virus or other malware for which specific antivirus software signatures are not yet available.
C&C attack communication channel is detected	Command and control attack communication channel is detected.
Critical vulnerability is detected	Critical vulnerability detected,
Endpoint FortiClient Telemetry is manually disconnected by user	FortiClient Telemetry endpoint is manually disconnected by user.
Endpoint signature database is out-of-date	Out-of-date endpoint signature is detected.
Endpoint software is out-of-date	Out-of-date endpoint software is detected.

4. Click *Save*.

   If you have not already set up an SMTP server, the GUI will automatically prompt you to configure the *SMTP Server Settings* information. See Configuring SMTP server settings on page 103.

Configuring SMTP server settings

You can set up an SMTP server to enable alerts for EMS events. When an alert is triggered, an email notification will be sent.

To configure SMTP server settings:

1. Go to *View* > *Settings* > *E-mail Alerts*, and enable *Send E-Mail Alerts for the Following EMS Events* or *Send e-mail alerts for the following endpoint events*.

   The *SMTP Server Settings* option is displayed under *Alerts*.

2. Click *SMTP Server Settings*, and set the following options:

SMTP Server		Enter the SMTP server.
Port		Enter the port number.
Security		Select *None*, *STARTTLS*, or *SMTPS* for the security type, or select the *Auto Detect* button to automatically select the security type. If *STARTTLS* or *SMTPS* is selected, the *Username* and *Password* boxes become available.
	Username	Enter the username.
	Password	Enter the password.
From Address		Enter the email address to send the alerts from.
Reply To		Enter the email address to send replies to.
Subject		Subject of the sent e-mail alert.
Recipients		Enter email address(es) to send alerts to. Click the + button to add more email addresses.
Test Email Settings		Click the button to test the configured email settings.

3. Click *Save*.

Alerts

Viewing alerts

You can view the alerts generated by FortiClient EMS. Examples of events that generate an alert include:

- New version of FortiClient is available
- FortiClient deployment failed
- Failure to check for signature updates
- Error encountered when downloading AD server entries
- Error encountered when scanning for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. It is cleared when you view the alert.

To view alerts:

1. Click the *Alert* icon (an envelope) in the toolbar. The *EMS Alert Logs* pane is displayed.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filter* to remove the filters.

Email alert settings

You can set up an SMTP server to enable alerts for EMS or endpoint events. When an alert is triggered, an email notification will be sent. For more information, see Configuring mail alert settings on page 102.

Creating a support package

To create a support package:

1. Go to *Help* > *Create Support Package*. The *Create Support Package* dialog box is displayed.
2. In the *Password* box, type your administrative password.
3. In the *Confirm Password* box, type your password again.
4. Click *Create Support Package*.